

Policy 5125: Student Records

Status: ADOPTED

Original Adopted Date: 03/01/2009 | **Last Revised Date:** 08/01/2026 | **Last Reviewed Date:** 08/01/2026

CSBA NOTE: The following mandated policy and accompanying administrative regulation address student records, which are governed by both federal and state law, including the Family Educational Rights and Privacy Act (FERPA) (20 USC 1232g, 34 CFR 99.1-99.8), the Protection of Pupil Rights Amendment (PPRA) (20 USC 1232h), the Children's Online Privacy Protection Act (COPPA) (15 USC 6501-6506, 16 CFR 312), Education Code 49069.7 and 49073.1, K-12 Pupil Online Personal Information Protection Act (Business and Professions Code 22584), Early Learning Personal Information Protection Act (Business and Professions Code 22586), and 5 CCR 430-438. For information regarding public access to certain records in accordance with the California Public Records Act (CPRA) (Government Code 7920.000 - 7930.215), see BP/AR 1340 - Access to District Records and BB 9012 - Board Member Electronic Communications. For information regarding retention of records, see BP/AR 3580 - District Records and AR 4112.6/4212.6/4312.6 - Personnel Files.

Pursuant to 5 CCR 431, districts are mandated to establish policies and procedures to implement state law and regulations regarding student records, including policies and procedures which (1) enumerate and describe the student records collected and maintained by the district, (2) ensure security of the records, and (3) guarantee access to authorized persons within five days of a request. Education Code 49069.7 mandates procedures related to review of student records by parent/guardian. See the accompanying administrative regulation for additional language implementing these mandates.

The Governing Board recognizes the importance of keeping accurate, comprehensive student records as required by law. The Superintendent or designee shall establish administrative regulations governing the identification, collection, retention, disclosure, and security of student records. These regulations shall ensure the rights of authorized persons to have timely access to student records while maintaining the confidentiality of student records in accordance with state and federal law.

The Superintendent or designee shall designate a certificated employee to serve as custodian of records with responsibility for student records at the district level. At each school, the principal or a certificated employee shall be designated as custodian of records for students enrolled at that school. The custodian of records shall be responsible for implementing Board policy and administrative regulation regarding student records. (5 CCR 431)

All appropriate personnel shall receive training regarding district policies and procedures for gathering and handling sensitive student information, including which information should not be solicited.

CSBA NOTE: Pursuant to Education Code 49076.7, a district is prohibited from soliciting or collecting social security numbers or the last four digits of social security numbers of students or their parents/guardians, unless otherwise required to do so by state or federal law. One such exception is the collection of the last four digits of the social security number for the purpose of establishing eligibility for a federal benefit program.

The district shall not collect or solicit social security numbers or the last four digits of social security numbers of students or their parents/guardians, unless otherwise required to do so by state or federal law. (Education Code 49076.7)

Records Related to Immigration or Citizenship Status

CSBA NOTE: Unless an exception applies, Education Code 234.7, as amended by AB 495 (Ch. 664, Statutes of 2025), prohibits the collection and disclosure of information or documents regarding the citizenship or immigration status of students or their family members. Additionally, the California Attorney General's July 2026 guidance, "Promoting Safe and Secure Government Access for All: Guidance and Model Policies to Assist State and Local Agencies in Responding to Immigration Issues Pursuant to Senate Bill 580 (2025)," provides recommendations, pursuant to SB 580 (Ch. 670, Statutes of 2025), for databases operated by state and local agencies to limit the availability of information in those databases for the purposes of immigration enforcement.

For more information regarding the prohibition against collecting and disclosing citizenship or immigration status of students or their family members, and limited exceptions, see BP/AR 1445 - Response to Immigration Enforcement and BP/AR 1340 - Access to District Records.

The immigration or citizenship status of a student or a student's family member may only be collected and disclosed in accordance with Board Policy and Administrative Regulation 1445 - Response to Immigration Enforcement.

The district or any district employee shall not compile a list, registry, or database based on students' national origin,

Policy 5125: Student Records

Status: ADOPTED

Original Adopted Date: 01/10/2019 | **Last Revised Date:** 05/13/2026 | **Last Reviewed Date:** 05/13/2026

The Governing Board recognizes the importance of keeping accurate, comprehensive student records as required by law. The Superintendent or designee shall establish administrative regulations governing the identification, collection, retention, disclosure, and security of student records. These regulations shall ensure the rights of authorized persons to have timely access to student records while maintaining the confidentiality of student records in accordance with state and federal law.

The Superintendent or designee shall designate a certificated employee to serve as custodian of records with responsibility for student records at the district level. At each school, the principal or a certificated employee shall be designated as custodian of records for students enrolled at that school. The custodian of records shall be responsible for implementing Board policy and administrative regulation regarding student records. (5 CCR 431)

If student records containing covered information which is not subject to the California Consumer Privacy Act are under the control of the operator of a website, online service or application, or mobile application, and the student's parent/guardian or the student, if 18 years of age or older, requests deletion of such records, the Superintendent or designee shall provide documentation to the operator that the student has not been enrolled in the district for at least 60 days. (Business and Professions Code 22584)

All appropriate personnel shall receive training regarding district policies and procedures for gathering and handling sensitive student information, including which information should not be solicited.

The district shall not collect or solicit social security numbers or the last four digits of social security numbers of students or their parents/guardians, unless otherwise required to do so by state or federal law. (Education Code 49076.7)

The immigration or citizenship status of a student or a student's family member may only be collected and disclosed in accordance with Board Policy/Administrative Regulation 1445 - Response to Immigration Enforcement.

The district or any district employee shall not compile a list, registry, or database based on students' national origin, ethnicity, or religious belief, practice, or affiliation, or disclose student information to federal government authorities for the purpose of compiling such a list, registry, or database for purposes of immigration enforcement. This prohibition does not apply to information that is aggregated and is not personally identifiable. (Government Code 8310.3)

The Superintendent or designee shall develop protocols to comply with a court's restraining order that prohibits a party from accessing specified records and information pertaining to a student. (Family Code 6323.5)

Student Records from Social Media

The Superintendent or designee may gather and maintain information from the social media of any district student, provided that the district first notifies students and parents/guardians about the proposed program, offers an opportunity for public comment at a regularly scheduled Board meeting, and gathers only information that directly pertains to school safety or student safety. (Education Code 49073.6)

Retention, Disclosure, and Security of Student Records

The Superintendent or designee shall ensure the confidentiality of student records as required by law and shall establish processes and procedures to safeguard data against damage, loss, or theft, including damage, loss, or theft which may be caused by the use of technology, including artificial intelligence and breaches to the district's digital infrastructure, in the retention or disclosure of student records.

The Superintendent or designee shall ensure that employees receive information and training about cybersecurity,

ethnicity, or religious belief, practice, or affiliation, or disclose student information to federal government authorities for the purpose of compiling such a list, registry, or database for purposes of immigration enforcement. This prohibition does not apply to information that is aggregated and is not personally identifiable. (Government Code 8310.3)

Family Court Records

CSBA NOTE: Pursuant to Family Code 6323.5, districts are required to develop protocols to comply with a court's restraining order that prohibits a party from accessing records and information pertaining to the education, day care, health care, recreational activities, or employment of a minor child of the parties, which may include prohibiting access to a parent/guardian who would otherwise be entitled to the records. The protocols must, at a minimum, (1) designate an appropriate employee(s) who is responsible for receiving protective order(s), (2) establish a means of ensuring that the restrained party is not able to access the prohibited records or information, and (3) implement a procedure for submitting a copy of the restraining order including confirmation of when and to whom it was submitted. It is recommended that districts with questions about complying with these procedures consult CSBA's District and County Office of Education Legal Services or district legal counsel.

The Superintendent or designee shall develop protocols to comply with a court's restraining order that prohibits a party from accessing specified records and information pertaining to a student. (Family Code 6323.5)

Student Records from Social Media

CSBA NOTE: Pursuant to Education Code 49073.6, any district considering a program to gather information from students' social media activity, as defined, is required to first notify students and parents/guardians and provide an opportunity for public comment. The notification may be provided as part of the annual parent/guardian notification required pursuant to Education Code 48980. If such a program is then adopted, the district is required to comply with program requirements reflected in "Student Records from Social Media" in the accompanying administrative regulation. If a district does not gather information from students' social media, the following section may be deleted.

It is recommended that the district consult CSBA's District and County Office of Education Legal Services or district legal counsel before gathering any other online information that does not meet the definition of social media in Education Code 49073.6.

The Superintendent or designee may gather and maintain information from the social media of any district student, provided that the district first notifies students and parents/guardians about the proposed program, offers an opportunity for public comment at a regularly scheduled Board meeting, and gathers only information that directly pertains to school safety or student safety. (Education Code 49073.6)

Retention, Disclosure, and Security of Student Records

CSBA NOTE: The use of artificial intelligence (AI) may pose risks to keeping student records private and secure. CSBA's, "Understanding Artificial Intelligence in K-12 Education: What Governance Teams Should Know," cautions districts to consider whether information about students shared with or stored in an AI-enabled system is subject to federal or state privacy laws and whether interactions between students and AI systems may create records that are required to be protected by law, such as when a chatbot or automated tutor generates written guidance to a student.

Pursuant to Education Code 33328.5, the California Department of Education (CDE) developed guidance on the safe use of AI in education and a model policy on the safe and effective use of AI. CDE's webpage, "Artificial Intelligence: Information regarding the role of artificial intelligence (AI) in California Public Schools," includes guidance for the safe and effective use of AI in schools, including data privacy, and a model policy. Regarding student records, the model AI policy states that (1) AI tools should protect student data, (2) AI usage should adhere to legal requirements including, but not limited to, FERPA, (3) education records or other confidential information should not be entered into AI tools unless expressly authorized under district policy, and (4) all AI vendor contracts should include enforceable provisions protecting student data privacy and security.

For more information on AI, see BP 0441 - Artificial Intelligence, BP/E(1) 4040 - Employee Use of Technology, BP 5131.9 - Academic Honesty, and BP/AR 6163.4 - Student Use of Technology.

The Superintendent or designee shall ensure the confidentiality of student records as required by law. Additionally, the Superintendent or designee shall establish processes and procedures to safeguard student records against damage, loss, or theft that may be caused by any technology used in the retention or disclosure of student records,

including artificial intelligence, or by a breach to the district's digital infrastructure.

The Superintendent or designee shall ensure that employees receive information and training about cybersecurity, including ways to protect student records from breaches to the district's digital infrastructure.

If the district experiences a cyberattack that impacts more than 500 students or personnel, the Superintendent or designee shall report the cyberattack to the California Cybersecurity Integration Center. (Education Code 35266)

CSBA NOTE: Education Code 49073.1 authorizes districts to enter into a contract with a third party for the digital storage, management, and retrieval of student records and/or for software designed for this purpose. A district that chooses to enter into such a contract is mandated to adopt policy allowing such contracts and is required to ensure that the contract includes all the provisions specified in Education Code 49073.1. For more information regarding contracts for digital storage and maintenance of student records, see BP 3312 - Contracts.

In accordance with law and Board Policy 3312 - Contracts, the Superintendent or designee may enter into a contract with a third party for the digital storage, management, and retrieval of student records and/or to authorize a third party provider of digital software to access, store, and use student records.

CSBA NOTE: The privacy of online information of students in prekindergarten (preK)-12 is addressed in Privacy Rights for California Minors in the Digital World (Business and Professions Code 22580-22582), the K-12 Pupil Online Personal Information and Protection Act (Business and Professions Code 22584-22585), and the Early Learning Personal Information Protection Act (Business and Professions Code 22586-22587). These statutes prohibit an operator of a website, online service or application, or mobile application from knowingly using, disclosing, or compiling the personal information of a minor for the purpose of marketing or advertising specified types of products or services; allowing a third party to use, disclose, or compile such information; or selling or disclosing specified student information or knowingly using such student information to engage in targeted advertising to students or parents/guardians or to amass a profile about a preK-12 student. Covered student information includes any personally identifiable information or materials created or provided by a student, parent/guardian, or district employee, such as name, contact information, educational record, discipline records, test results, health records, and socioeconomic information. Pursuant to Business and Professions Code 22584 and 22586, an operator is required to delete data under the control of the school or district upon the request of the school or district.

Additionally, pursuant to Business and Professions Code 22584 and 22586, upon request by a student's parent/guardian or the student if 18 years of age or older, such operator is required to delete the student's covered information that is under the operator's control but which is not subject to the California Consumer Privacy Act (Civil Code 1798.100 - 1798.199.100).

However, Business and Professions Code 22584 and 22586 do not require the deletion of student records held by a national assessment provider when the records only include standardized test results, mandatory permanent student records, and any official records or files directly related to a student and maintained by the operator, school, or district.

The operator of a website, online service or application, or mobile application that controls such student record shall delete any student data under the control of the school or district upon request by the district. Additionally, the student's parent/guardian, or the student if 18 years of age or older, may request the operator to delete any student's records containing covered information which is not subject to the California Consumer Privacy Act. (Business and Professions Code 22584, 22586)

including ways to protect student records from breaches to the district's digital infrastructure.

If the district experiences a cyberattack that impacts more than 500 students or personnel, the Superintendent or designee shall report the cyberattack to the California Cybersecurity Integration Center. (Education Code 35266)

The Superintendent or designee may enter into a contract with a third party for the digital storage, management, and retrieval of student records and/or to authorize a third party provider of digital software to access, store, and use student records, provided that the contract meets the requirements of Education Code 49073.1 and other applicable state and federal laws
