CALIFORNIA

Student Data Privacy and Security Highlights

California laws and regulations reflect and supplement FERPA's access and disclosure requirements applicable to education records held by school districts, the California Department of Education, and other education entities. California's student data protections generally align with federal student privacy requirements to safeguard personally identifiable information and to ensure each student's privacy and confidentiality. These education laws expressly prohibit, with some exceptions, school districts from disclosing personally identifiable information without consent while also providing the student's parents and eligible students the right to access their own records.

This section highlights key California protections for student data but does not provide a comprehensive list or description of the state's statutory and regulatory privacy requirements. Readers should always consult their local counsel for further information about California and federal laws applicable to student data.

FERPA FAQs

1. Does California law and regulation specifically address FERPA's requirements?

SHORT ANSWER: Yes. California incorporates the privacy requirements of FERPA by limiting access to pupil records, as well as other federal and state laws that safeguard education records, privacy, and confidentiality.

DEEPER DIVE: Several sections of California student privacy law specifically reference FERPA. California statute states that "[a] school district shall not permit access to pupil records to a person without written parental consent or under judicial order except [...] as permitted by [FERPA's regulations]."[1] Directory information of a homeless child or youth may not be released "unless a parent, or pupil accorded parental rights, as identified in the federal Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g), has provided written consent that directory information may be released."[2] Additionally, California has a longitudinal pupil data systems referred to as CALPADS. State law allows for CALPADS data to be available and accessible to researchers "in a manner that complies with federal and state privacy laws, including but not limited to, the Family Educational Rights and Privacy Act."[3]

2. Does California law limit access to personally identifiable student records?

SHORT ANSWER: Like FERPA, California law limits access to pupil records. Covered student information may only be released with parental consent, judicial order, or under other limited circumstances.

DEEPER DIVE: Each school district is responsible to establish written policies and procedures to ensure the security of pupil records and provide for authorized persons to get access to such records.[4]

Written parental consent or judicial order is required in order to obtain access to pupil records. Certain other limited exceptions apply to the release of pupil records without consent, including release to school officials and employees of the school district, officials and employees of other districts where the student intends to enroll, authorized representatives of government agencies, a pupil 16 years of age or older or having completed the tenth grade, attorneys where the information will be used in cases involving the particular student, and certain other specific individuals.[5] This statute also allows for release of information if the records or information are deidentified. Under California statute, the State Superintendent and state board may also approve additional prohibitions on the collection of other personally identifiable information.[6]

California prohibits school districts, offices of education, and charter schools from collecting or soliciting social security numbers or the last four digits of social security numbers from students unless it is required by law.[7] Parents may provide written consent for the release of student information, provided the receiving party is identified and the recipient is notified that the transmission of the information to others without the additional written consent of the parent is prohibited.[8]

3. Does California place restrictions on FERPA's "directory information" exception?

SHORT ANSWER: Yes. Consistent with FERPA, school districts are allowed to adopt policies that identify which categories of directory information may be released and to whom the information may be released with several limitations. Further the school district is allowed to determine which individuals, officials, or organizations may access the directory information. State law prohibits, however, releasing directory information to a profitmaking entity.

DEEPER DIVE: California law requires school districts to "adopt a policy identifying those categories of directory information [...] that may be released."[9] Further, "directory information" has been defined to include a pupil's name, address, telephone number, date of birth, email address, major field of study, participation in officially recognized activities and sports, height and weight of a member of an athletic team, dates of attendance, degrees and awards, and most recent previous public or private school attendance.[10]

In addition to determining what information will be categorized as "directory information," school districts in California may also determine which individuals, officials, or organizations may access the directory information. This information, however, may not be released to a private profitmaking entity, which may include newspapers, magazines, and radio stations. California may also limit or deny certain types of directory information to public or private nonprofit organizations if it is in the best interests of pupils.[11]

School districts in California must annually provide a privacy notice to parents which must include what information will be released and the recipients of such information, and if a parent objects to releasing the information, the directory information shall not be released.

4. Does California provide a model data security plan for school districts?

SHORT ANSWER: No. However, the California Department of Education has a data governance program that provides information and guidance to educators who seek to maintain data governance and security at the local level.

DEEPER DIVE: The California Department of Education utilizes an Education Data Governance program that develops and supports data-related policies, procedures, roles, and responsibilities.[12] This program provides tools for educators and school districts to work to establish data governance at the local level. One goal of this program is to "[i]ncrease Educational Data Quality and Standardization by supporting CDE staff and local educational agencies (LEAs) in understanding, interpreting, and complying with standards, reporting requirements, and data use best practices."[13]

5. Does California place special data privacy requirements on third parties that work with schools?

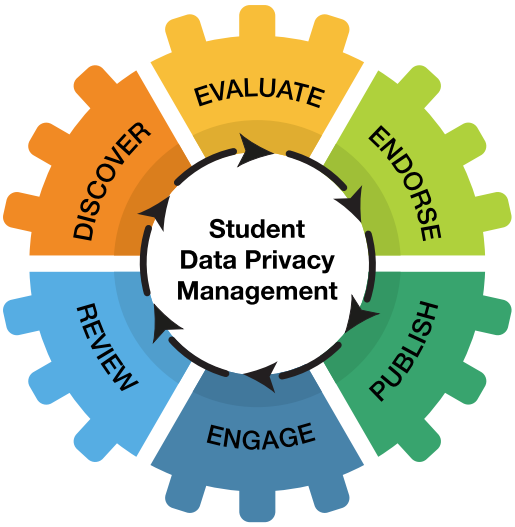
SHORT ANSWER: Yes. California law prohibits "operators" from selling a student's personally identifiable information, using it for targeted advertising, or amassing student profiles. The law also requires operators to meet other specific privacy requirements.

DEEPER DIVE: California law allows local educational agencies to enter into contracts with third parties in order to provide services to the school or to provide digital educational software. Any local educational agency that enters into these third-party contracts must follow certain requirements, including prohibiting the third party from "using any information in the pupil record for any purpose other than those required or specifically permitted by the contract."[14] These contracts must also include a description of how the parties will jointly ensure compliance with FERPA. California law also places limits on programs that gather or maintain records that include information obtained from social media accounts of students at the school.[15]

California law places limits on "operators" who access student online personal information through the *Student Online Personal Information Protection Act*.[16] "Operators" are defined as the "operator of an Internet Web site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes."[17]

Operators are prohibited from knowingly engaging in targeted advertising, using information to amass a profile about a K-12 student in furtherance of K-12 school purposes, or selling student information including covered information. Operators are also prohibited from disclosing information unless the disclosure is made in furtherance of the K-12 purpose of the site, to ensure legal and regulatory compliance, to respond to a judicial process, to protect the safety of users, or to another service provider under certain limited circumstances. Any operator is also required to implement and maintain "reasonable security procedures and practices" and delete information when requested by the school or district. Operators are allowed to use student information under certain limited circumstances, including for legitimate research purposes as well as with some limitations when the information has been deidentified, for example to demonstrate the effectiveness of an operator's products and services. Finally, there is nothing in law that prohibits an operator from sharing "aggregated deidentified student covered information" in order to develop and improve educational services.[18]

DEEPER Conversations to Support Student Data Privacy Policy Compliance



DISCOVER new and existing district application usage

EVALUATE application privacy policies, terms of service, and 3rd party policy badging

ENDORSE approved apps by grade, building, or district

PUBLISH list of approved apps, policies, contracts and more with stakeholders

ENGAGE leadership in ongoing conversations on effective usage, results, and application efficacy

REVIEW policy changes, compliance, and application updates

CatchOn allows you to engage your entire leadership team in DEEPER conversations to safeguard your student data and help maintain compliance with state and federal privacy laws.

A few questions your district should consider when selecting a tool to monitor student data privacy compliance:

1. How are you discovering and tracking those apps and online tools your students are using on your school-owned devices that are unknown, not approved, and/or lie outside of your SSO?
2. If you are using an analytics tool to track usage, does that analytics tool allow you to review application information including privacy policies, terms of service, and 3rd party approvals from privacy consortiums like Student Data Privacy Consortium and IMS Global?
3. Does your analytics tool notify you of application policy updates automatically?
4. Are you able to tag your applications for approved use at various grade, building or program level usage?
5. Can you share your application information and privacy policies publicly with district and community stakeholders?
6. Will your analytics tool allow you to see trending application usage within your district, as well as other districts, and monitor accurate application usage by students to the minute with an active window monitoring feature?

CatchOn's Commitment to Promoting Student Data Privacy

CatchOn proudly supports and has signed the Student Privacy Pledge. As a software as a service solution that is both a software discovery and usage tracking tool for applications, CatchOn is committed to protecting student data. Our 360-degree approach to student data privacy helps you keep your data safe and provides you real-time visibility into the learning tools being used in your school district.

See how CatchOn specifically helps districts stay compliant with education privacy laws below.

Education Law What is Required at a Glance	**CatchOn's Solution** How CatchOn Can Help You Stay Compliant	
Review 3rd party agreements	Affords quick access to 3rd party websites and privacy policies	✓
Ensure District privacy/security policies are aligned	Provides ability to mark and categorize applications as approved or not approved by the district	✓
District data protection office	Enables education leaders to see software applications used on school devices, both inside and outside the classroom; Empowers leaders to diagnose applications vulnerable to student data privacy policies	✓
Continuous review for compliance	Provides the ability to monitor known and unknown apps for compliance	✓
Parental notifications	Enables districts to post and share approved and monitored apps with parents using automated reports	✓
Breach notification plan	Provides the ability to gather data on EdTech usage, applications privacy policies, and district purchases to avoid vulnerabilities	✓
Align to NIST framework and FERPA policies	CatchOn tracks only de-identified aggregated information PII stays on district server; CatchOn signed student privacy pledge	✓
Privacy training	Enables districts to facilitate training opportunities by leveraging data analytics that track data usage, trends, and impact	✓

[1] Cal. Ed. Code 49076(a) (citing FERPA regulations).
[2] Cal. Ed. Code 49073.
[3] Cal. Ed. Code 49079.5.
[4] CCR 431 Responsibilities of Local Governing Boards.
[5] Cal. Ed. Code 49076.
[6] Cal. Ed. Code 49076.7.
[7] Cal. Ed. Code 49076.7.
[8] Cal. Ed. Code 49075.
[9] Cal. Ed. Code 49073(a).
[10] Cal. Ed. Code 49061(c).
[11] Cal. Ed. Code 49073(a).
[12] California Department of Education, Educational Data Governance. https://www.cde.ca.gov/ds/ed/index.asp.
[13] California Department of Education, Educational Data Governance, EDGO Goals. https://www.cde.ca.gov/ds/ed/index.asp.
[14] Cal. Ed. Code 49073.1.
[15] Cal. Ed. Code 49073.6.
[16] Cal. Bus. & Prof. Code 22584.
[17] Cal. Bus. & Prof. Code 22584(a).
[18] Cal. Bus. & Prof. Code 22584.

Provided by:

An ENA Affiliate
catchon®

CatchOn is an expansive data analytics tool that compiles real-time data on every device, enabling school districts to make data-informed decisions about the apps and online tools their educators and students are using. In 2018, CatchOn joined forces with ENA, a leading provider of comprehensive technology solutions to education institutions and libraries across the nation. Collectively, CatchOn and ENA leverage their respective resources and expertise to deliver critical services and solutions that help school districts produce positive outcomes in the communities they serve. For more information, please visit www.catchon.com, call **866-615-1101**, or email **solutions@catchon.com**

FORESIGHT LAW+POLICY

Foresight Law + Policy is a national education law firm based in Washington, D.C. Our lawyers and other professionals counsel education leaders, nonprofit organizations and companies working to strengthen public education and prepare all kids for success. For more information, please visit https://www.flpadvisors.com/

Contributing Author:
Reg Leichty, Founding Partner

SETDA
LEADERSHIP • TECHNOLOGY • INNOVATION • LEARNING

Founded in 2001, the **State Educational Technology Directors Association (SETDA)** is the principal nonprofit membership association representing US state and territorial educational technology leaders. Our mission is to build and increase the capacity of state and national leaders to improve education through technology policy and practice. For more information, please visit setda.org.