COLORADO

Student Data Privacy and Security Highlights

Colorado's Student Data Transparency and Security Act supplements federal privacy protections for student personally identifiable data.[1] The Student Data Transparency and Security Act's requirements apply to the Colorado Department of Education and other "local education providers," including school districts, district or state authorized charter schools, and any board of cooperative services that operates one or more public schools. Separately, Colorado law provides statutory protections for for the personally identifiable information of teachers related to their evaluations, licensure, and authorizations.[2]

This section highlights these Colorado requirements and their relationship to related federal laws, including the Family Educational Rights and Privacy Act (FERPA); however, school districts covered by the Student Data Transparency and Security Act should consult their local counsel for further information about how to comply fully with the law and other Colorado and federal privacy requirements applicable to student data.

FERPA FAQs

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

SHORT ANSWER: Yes. The Student Data Transparency and Security Act requires the State Board of Education to develop and make publicly available policies and procedures to comply with FERPA and other privacy laws and policies.[3]

DEEPER DIVE: The Student Data Transparency and Security Act requires the State Board of Education (SBE) to publish privacy policies and procedures "to comply with the Federal 'Family Educational Rights and Privacy Act of 1974' and other relevant Privacy Laws and Policies [...]." By law, the SBE was required to create policies that limit access to Colorado's Student Data System to the following:

- Authorized Department of Education and Office of Information and Technology staff that require such access
- The Department of Education's contractors that require access to the system to perform their duties
- School district administrators, teachers, and school personnel who require access to perform their duties
- Students and parents
- The authorized staff of other state agencies, including public institutions of higher education, as required by law or defined by inter-agency data-sharing agreements[4]

2. Does Colorado privacy law include specific requirements for school districts?

SHORT ANSWER: Yes. Among other requirements, school districts must publicly describe the student data they collect and how the information is used and shared. This requirement includes providing information about school district contractors who have access to data. School districts must also adopt and publish privacy policies and review the policies at least annually.

DEEPER DIVE: Every Local Education Provider, including school districts, district- or state-authorized charter schools, and any board of cooperative services that operates one or more public schools, must post an explanation online of the student personally identifiable information it collects and maintains as well as how the information is used and shared. The notice must also list the School Service Contract Providers that it works with and post a copy of the contract governing these relationships. Contracts with service providers must require their compliance with relevant provisions of the Student Data Transparency and Security Act. Each Local Education Provider must also adopt a student information privacy and protection policy that addresses specific requirements described by the statute. This policy must be reviewed annually, made available to parents, and posted on the Local Education Provider's website.[5]

3. Does Colorado law prohibit data sales and provide other special requirements for third party service providers?

SHORT ANSWER: Yes. The Student Data Transparency and Security Act prohibits the Department of Education from selling, trading, gifting, or monetizing student personally identifiable data.[6] School Service Contract Providers are also prohibited from selling student data, using it for advertising, or creating student profiles not required by the contract.

DEEPER DIVE: School Service Contract Providers are entities with formal contracts to provide "school services" such as Internet websites, online services, online applications, or mobile applications to Public Education Entities. Public Education Entities include school districts, BOCES that operate one or more schools, charter schools, the Colorado Department of Education, the State Charter School Institute, and traditional public schools. School Service Contract Providers are prohibited from selling student personally identifiable information, using student personally identifiable information for targeted advertising, or creating a student profile unless the profile is a required component of the contract. School Service Contract Providers must also provide clear information explaining the data elements they collect, the learning purpose for which it is collected, and how the provider uses and shares the information. Among other requirements, School Service Contract Providers must also notify the education entities they work with before changing their privacy policies, provide notice of misuse or unauthorized release of data (including by subcontractors), and destroy protected student data at the conclusion of the contract.[7]

4. Does Colorado law address student data security plans?

SHORT ANSWER: Yes. Colorado's Student Data Transparency and Security Act directs the State Board of Education to develop "a detailed data security plan" that includes guidance for authorizing access to the student data system; privacy compliance standards; privacy and security audits; security breach planning, notice, and procedures; student personally identifiable information retention and destruction policies; guidance for school districts and staff regarding student personally identifiable information use; consequences for security breaches; and staff training regarding the policies.[8] The statute also requires the Department of Education to "develop data security guidance" that may be used by Local Education Providers and specifies elements that must be reflected in the guidance.[9]

DEEPER DIVE: The Department of Education's data security guidance must include recommendations for authorizing access to the state's student data system and to student personally identifiable information; authenticating authorized access; privacy compliance standards; best practices for privacy and security audits; breach planning, notice, and procedures; data retention and destruction procedures; collection and sharing procedures; ensuring contracts associated with databases, assessments, or instructional supports include provisions to safeguard privacy and security; outsourcing of educational services; online education; publishing a list of local education vendors; consequences for security breaches; and staff training.[10] Colorado law also requires all government agencies, including the Colorado Department of Education, to maintain an information security policy and plan. The Colorado Department of Education also monitors all access and access attempts to all of its data systems and maintains a centralized authentication and authorization process to further track access and safeguard personally identifiable information.[11]

5. Does Colorado law address student data privacy and security training?

SHORT ANSWER: Yes. Colorado law requires the State Board of Education to develop a "detailed data security plan" that includes a focus on "staff training" regarding the policies.[12]

DEEPER DIVE: The Department of Education's Information Management Systems Policies and Procedures note that all new department employees and contractors must sign acceptable use policies and confidentiality agreements as well as participate in annual "information security and privacy fundamentals training." The Department of Education also provides privacy training and guidance to local school districts about complying with state and federal privacy laws and best practices.[13]

6. Does Colorado offer model privacy policies for school districts and schools?

SHORT ANSWER: Yes. The Student Data Transparency and Security Act requires the Colorado Department of Education to provide a model Student Information Privacy and Protection Policy for school districts, district- or state-authorized charter schools, and any board of cooperative services that operates one or more public schools.

DEEPER DIVE: The Student Data Transparency and Security Act requires the Colorado Department of Education to develop and publish a model Student Information Privacy and Protection Policy. By law the sample policy must include protocols for creating and maintaining a student data index; retaining and destroying student personally identifiable information; using student personally identifiable information for purposes internal to a local education provider; preventing breaches in the security of student personally identifiable information and for responding to any security breaches that occur; contracting with school service contract providers and using school services provided by school service on-demand providers; disclosing student personally identifiable information to school service contract providers, school service on-demand providers, or other third parties; notifying parents regarding collection of, retention of, and access to student personally identifiable information; and providing training in student information security and privacy to employees of a local education provider.[14]

A wide array of sample privacy and security policies are available on the Colorado Department of Education website.[15]

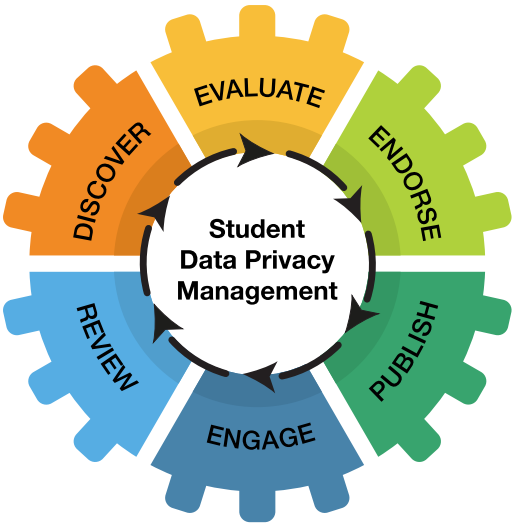
7. Does Colorado law protect educator evaluation records?

SHORT ANSWER: Yes. Colorado law protects personnel records, including records associated with mandatory teacher and leader evaluations, from public disclosure.

DEEPER DIVE: "[T]he evaluation report and all public records [...] used in preparing the evaluation report shall be confidential and shall be available only to the licensed person being evaluated, to the duly elected and appointed public officials who supervise his or her work, and to a hearing officer conducting a hearing [...]."

Additionally, "[a] school district or board of cooperative services may use the information collected to fulfill its duties as required by law [...]. In such instances, the identity of individual educators or students, including but not limited to student assessments results linked to the individual educator, must otherwise remain confidential and must not be published or publicly disclosed in any way that would identify an individual educator."[16]

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] C.R.S. 22-16-101 et seq.
[2] C.R.S. 22-2-111; C.R.S. 22-9-109.
[3] C.R.S. 22-16-104(b).
[4] Ibid; See also guidance related materials on the Colorado Department of Education website, available at https://www.cde.state.co.us/dataprivacyandsecurity-0.
[5] C.R.S. 22-16-107.
[6] C.R.S. 22-16-105(3)(d).
[7] C.R.S. 22-16-109; C.R.S. 22-16-110.
[8] C.R.S. 22-16-104(d).
[9] C.R.S. 22-16-106(1).
[10] Ibid.
[11] C.R.S. 24-37.5-404.
[12] C.R.S. 22-16-104.
[13] Ibid; See also Colorado Department of Education - Information Management Systems Policies and Procedures: Personally Identifiable Information Protection, available at https://www.cde.state.co.us/sites/default/files/docs//Personally%20Identifiable%20Information%20Protection%20Policy%2008.2019_New%20Branding.pdf.
[14] C.R.S. 22-16-106(2)(a-h).
[15] Colorado Department of Education Sample Privacy and Security Policies, available at https://www.cde.state.co.us/dataprivacyandsecurity/sampleitpolicies.
[16] C.R.S. 22-9-109.

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.