GEORGIA

Student Data Privacy and Security Highlights

Georgia provides parents and students with the right to access and review the student's education records, limits local and state personally identifiable information disclosures, promotes transparency about the state's student data inventory and uses, and prohibits data sales and targeted advertising by certain companies that work with schools. State law also requires the Georgia Department of Education to designate a chief privacy officer and establish "department-wide" privacy policies related to the "use, collection, and disclosure of student data."

This summary highlights and provides general information about these and other Georgia student data protections but does not provide a comprehensive list of the state's statutory and regulatory privacy requirements applicable to students. Readers should consult local counsel for definitive information about Georgia's student privacy laws.

FERPA FAQs

1. Does Georgia provide parents and students with specific rights related to a student's education records?

SHORT ANSWER: Yes. Georgia provides parents and students with the right to inspect and review their education records and challenge inaccurate content.

DEEPER DIVE: Georgia law grants parents the "right to inspect and review his or her child's education record maintained by the school or local board of education." A parent can also request—from the school or local board of education—data in the child's education record, including data maintained by specified outside companies ("operators") working with the schools. Local boards must provide the parent or guardian with an electronic copy of the record upon request unless it is not maintained in electronic format and reproducing an electronic version would be "unduly burdensome." A parent or eligible student also has the right to request corrections to inaccurate information contained in the education record.[1]

2. Does Georgia limit disclosures of a student's personally identifiable student data?

SHORT ANSWER: Yes. Under Georgia regulations, a student's personally identifiable data may not be disclosed without parent consent, except as permitted by the Family Educational Rights and Privacy Act (FERPA).

DEEPER DIVE: Georgia education regulations prohibit a student's personally identifiable information from being disclosed without parent consent. However, there are a number of exceptions to this general rule. The state's regulations adopt the unconsented-to disclosure exceptions provided by FERPA, such as to school officials with legitimate educational purposes; to other schools or postsecondary institutions where the student intends or seeks to enroll; and for financial aid purposes, for auditing and evaluating federal programs, and other listed options.[2]

3. Does Georgia law place special privacy requirements on the Georgia Department of Education?

SHORT ANSWER: Yes. Georgia law requires the state superintendent to appoint a chief privacy officer and requires the state to adopt security protocols and practices. Generally, student personally identifiable data may not be redisclosed by the Georgia Department of Education except in limited cases.

DEEPER DIVE: State law specifies that the Georgia Department of Education shall not transfer a student's personally identifiable data to any federal, state, or local agency or nongovernmental organization unless otherwise provided by law or approved by the State Board of Education.

Georgia permits the state education agency to disclose student data in the following situations:

- Students transferring to schools within the state or out of state
- Students enrolling in postsecondary institutions or training programs
- Registration for state, national, or multistate assessments
- Voluntary participation in a program for which such data transfer is a condition or requirement in order for the student to participate
- Student data transfers for federal program purposes when the student is classified as a migrant
- Audits, compliance reviews, or complaint investigations by federal agencies
- At the request of the student or student's parents/legal guardians[3]

4. Does Georgia law limit the information that schools can share with the state's department of education?

SHORT ANSWER: Yes. Georgia law specifies that some sensitive student records should not be reported to the Georgia Department of Education.

DEEPER DIVE: Georgia expressly prohibits schools and local boards of education from reporting juvenile delinquency records, criminal records, and medical and health records to the Georgia Department of Education. Georgia law prohibits, unless otherwise required by state or federal law or in cases of health or safety emergencies, school districts from collecting the following information on students or their families: political affiliation, voting history, income, and information about religious affiliation or beliefs.[4]

5. **Does Georgia have a State Longitudinal Data System (SLDS) and is it governed by specific privacy requirements?**

SHORT ANSWER: Yes. Georgia has a SLDS that links to school districts' student information systems. The SLDS is governed by specific state privacy requirements.

DEEPER DIVE: State law requires the Georgia Department of Education to "create, publish, and make publicly available a dictionary of data elements with definitions of student personally identifiable data fields."[5] The Department of Education must make public the policies and procedures used to ensure the SLDS's operations comply with "applicable state and federal data privacy and security laws" including FERPA. The policies and procedures must at a minimum include limitations on accessing the data system except by authorized parties such as students and parents, district administrators, teachers, and authorized state agency staff.[6]

6. **Does Georgia law prescribe data security requirements for the state and school districts?**

SHORT ANSWER: Yes. The state requires the Georgia Department of Education to develop a security plan for the state data system and to provide security guidance to local school boards that is consistent with the state plan.

DEEPER DIVE: State law specifies that the Department of Education shall create the following:

- A data security plan for the state data system in order to limit who has access to student data
- Information on privacy and security audits
- Plans for security breaches, data retention, and data disposal
- Data security training
- Standards on aggregated data and guidance for local boards to implement effective security practices that are consistent with those of the state data system[7]

7. **Does Georgia law require the Department of Education to develop other model policies focused on student privacy?**

SHORT ANSWER: Yes. Georgia law requires the Department of Education to develop model privacy policies for local boards of education and schools.

DEEPER DIVE: The Department of Education is required to develop model policies for local boards of education to help them fulfill their student data privacy responsibilities. The model policies must include policies on the following:

- Annually notify parents about their rights to access student information
- Ensuring security when providing student data to parents
- Properly providing data only to authorized individuals
- Using technologies and programs to allow a parent to view online, download, and transmit data specific to his or her child's education record.

The Department must also establish model policies and procedures for a parent or eligible student to file a complaint if there has been a violation of rights under both federal and state student data privacy and security laws.

8. Does Georgia law provide specific protections for student data shared by schools with other public entities and companies?

SHORT ANSWER: Yes. Georgia's Student Data Privacy, Accessibility, and Transparency Act (SDPATA) aims to ensure that student data is safeguarded and that student privacy is protected.[8] Among other provisions, the SDPATA governs sharing data by schools with certain third party companies ("operators"), including prohibiting covered companies from selling student data or using it for targeted advertising.

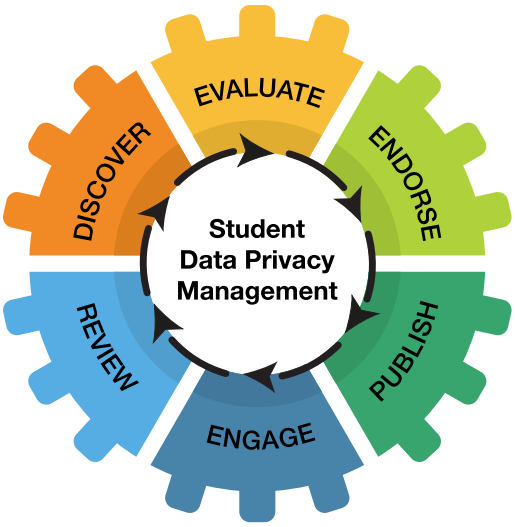
DEEPER DIVE: Georgia law prohibits "operators" from using student data to engage in targeted advertising, using information to create profiles about a student, selling student data, or disclosing student data without consent. Operators are outside entities that provide an Internet website, online service, online application, or mobile application to schools; know their products or services are designed for and used for K-12 school purposes; and collect, maintain, or use student data.

Operators may disclose student information for an educational, public health, or employment purpose if this is requested by the student's parent or guardian. Operators may disclose student information without consent by the student or student's parents or guardian provided the disclosure is only made for the following purposes and meets certain other limitations:

- In furtherance of a K-12 school purpose, with certain limits
- To ensure legal or regulatory compliance or protect against liability
- To respond to or participate in the judicial process
- To protect the security or integrity of the entity's website, service, or application
- To protect the safety of users or security of the site
- To another service provider, provided certain requirements are met

Georgia law also provides for certain other enumerated disclosure exceptions, including for legitimate research purposes; for purposes related to the operator's site, service, or application; and for adaptive learning or customized learning purposes, among others.[9]

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] O.C.G.A. § 20-2-667; See also Ga. Comp. R. & Reg. § 160-4-7-.08
[2] Ga. Comp. R. & Reg. § 160-4-7-.08
[3] O.C.G.A. § 20-2-664(3).
[4] O.C.G.A. § 20-2-665.
[5] O.C.G.A. § 20-2-664(1). Examples of student data elements that are collected are available at: Georgia Department of Education – SY18-18 Student Data Elements, https://www.gadoe.org/Technology-Services/Data-Collections/Documents/Data%20Collection%20Website/FY2019/SY18-19%20Data%20Element%20for%20posting.pdf.
[6] O.C.G.A. § 20-2-664(2).
[7] O.C.G.A. § 20-2-664(4).
[8] O.C.G.A. § 20-2-661.
[9] O.C.G.A. § 20-2-666.

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.