

ILLINOIS

Student Data Privacy and Security Highlights



Illinois' student data privacy laws integrate and build on the requirements of the Family Educational Rights and Privacy Act (FERPA). Among other privacy provisions, Illinois law

- Requires school districts to provide parents and students with the ability to review and correct their education records
- Describes which parties may access student's personally identifiable data and for what purposes
- Requires schools to designate a data custodian and secure and protect data.

Illinois law also prohibits specified entities that work with schools or school districts from: selling or renting a student's personally identifiable data; using student data for targeted advertising; and amassing student profiles for a non-educational purpose.

This informational resource highlights these and other Illinois protections for student data but does not provide a comprehensive explanation of the state's statutory and regulatory privacy requirements. Readers should consult their local counsel for further information about Illinois law.

FERPA FAQs

1. Does Illinois limit access to a student's personally identifiable student data?



SHORT ANSWER: Yes. Under Illinois law, a student's personally identifiable data may not be released, transferred, disclosed, or disseminated, except in limited circumstances.

DEEPER DIVE: Illinois prohibits a student's records from being disclosed without written consent. There are several exceptions, however, to this general rule. Students records may be released without consent to the following parties:

- A parent or student
- An employee or official of the school or school district or State Board with a current demonstrable educational or administrative interest
- The official records custodian of another school in which the student has enrolled or intends to enroll
- Any person for the purpose of research, statistical reporting, or planning
- Pursuant to a court order

- Any person if it is required by state or federal law
- Juvenile authorities when necessary for the discharge of official duties
- In connection with an emergency, if it is necessary to protect the health or safety of the student or other persons
- Any person with prior written parent consent
- A governmental agency, or social service agency with a contract with a governmental agency, in furtherance of an investigation of a student's school attendance
- Certain committee members for the purposes of identifying serious habitual juvenile offenders
- Department of Healthcare and Family Services
- The State Board or another state government agency in order to evaluate or audit federal and state programs.

Each person or entity that lawfully received the data must ensure that no other person has access to the information without prior consent.¹

2. Does Illinois govern researchers' access to personally identifiable student data?



SHORT ANSWER: Yes. Illinois allows researchers to access personally identifiable student information, but such disclosure must satisfy FERPA's requirements. Researchers seeking personally identifiable data from the Illinois Department of Education must also meet additional state requirements.

DEEPER DIVE: Illinois specifies that student data may be released by school districts or the state for research, statistical reporting, or planning, provided that these actions are permissible under and in accordance with FERPA.²

In other words, researchers must satisfy FERPA's data disclosure exception for qualified "studies" or the exception for an "audit or evaluation of state or federal programs." The Illinois State Boards of Education's Data Access and Use Policy and Procedures requires researchers seeking student data at the state level to take additional administrative steps. Researchers must meet all application requirements in the state's Instructions for Researchers Requesting Data forms, the research must be approved by the Illinois State Board of Education's Data Request Review Board, the researcher must acknowledge the confidentiality requirements of the research and sign a form, and the recipient of the student data must enter into a written data sharing agreement with the Illinois State Board of Education.³

3. Does Illinois law permit the release of directory information without parent or student consent?



SHORT ANSWER: Yes. Illinois law and regulations permit the release of certain student personally identifiable data that has been properly classified as directory information, but parents must be given notice of the school's plan to designate eligible data as directory information and parents must be provided an opportunity to opt out of the data's release.⁴

DEEPER DIVE: Illinois regulations provide that directory information "may be released to the general public, unless a parent requests that any or all the directory information not be released on his/her child. School districts shall notify parents annually of the information that is considered to be 'directory information' and of the procedures to be used by parents to request that specific information not be released."⁵

Only the following types of information may be designated as directory information under Illinois law:

- Identifying information: student's name, address, grade level, and birth date and place; parents' names, mailing addresses, electronic mail addresses, and telephone numbers
- Photographs, videos, or digital images used for informational or news-related purposes of a student participating in school or school-sponsored activities, organizations, and athletics that have appeared in school publications, such as yearbooks, newspapers, or sporting or fine arts programs, with some exceptions
- Academic awards, degrees, and honors
- Information in relation to school-sponsored activities, organizations, and athletics
- Major field of study
- Period of attendance in the school⁶

4. Does Illinois require schools and districts to protect and prevent unauthorized access to student records?



SHORT ANSWER: Yes. Illinois requires schools to designate official records custodians who are tasked with ensuring the security of student records.

DEEPER DIVE: Illinois requires schools to designate custodians who are responsible for the maintenance, care, and security of all school student records. The records custodian must take all “reasonable measures to prevent unauthorized access to or dissemination” of student records. Illinois schools must also take steps to ensure that only information that is clearly relevant to the education of a student is contained in the student's school record. If a school chooses to destroy or delete information in a student record, the parent or the student shall be given notice and an opportunity to make a copy of the records and information prior to destruction or deletion.⁷

5. Does Illinois law provide parents and students with specific rights related to a student's education records?



SHORT ANSWER: Yes. Illinois law and regulations provide parents and students with the right to inspect and copy the records, challenge the contents of the records, and limit any consent to designated records or designated portions of information within the records.

DEEPER DIVE: Illinois law requires the State Board of Education to issue regulations to govern the contents of student records.⁸ The law provides the following rights to parents and students:

- Students and parents have the right to inspect and copy all student records⁹
- Student records or information are not released, transferred, disclosed, or otherwise disseminated, except in certain enumerated circumstances¹⁰
- Parents may challenge the accuracy, relevancy, or propriety of entry into student records¹¹
- Access to procedures for filing a grievance action for violation of the Student Records Act¹²

6. Does Illinois have a centralized state data system that houses all student data information?



SHORT ANSWER: Yes. The Illinois State Board of Education, Illinois Community College Board, and the Illinois Board of Higher Education have an agreement to share information pursuant to the P-20 Longitudinal Education Data System Act.

DEEPER DIVE: Illinois has a statewide longitudinal data system (SLDS) and data warehouse that links “early learning, elementary, and secondary school student unit records with institution of higher learning student unit records.”¹³ State law limits the collection, use, maintenance, disclosure, and sharing of this data, including requiring the Department of Education to adopt procedures to protect student information in the SLDS from the intentional or accidental release of information.

7. Does Illinois place special data privacy requirements on the third parties that work with schools?



SHORT ANSWER: Yes. The state’s Student Online Personal Protection Act (SOPPA) prohibits “operators” that work with schools or school districts from selling or renting student personally identifiable data, using it for targeted advertising, or amassing student profiles. The law also requires operators to meet other specific privacy obligations.

DEEPER DIVE: SOPPA places limits on “operators” who access student data in the course of working with schools and school districts.¹⁴ “Operator” means an “operator of an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K through 12 school purposes and was designed and marketed for K through 12 school purposes.”¹⁵

Operators may not engage in targeted advertising using any information that the operator has acquired through K-12 purposes, which are defined as “purposes that are directed by or that customarily take place at the direction of a school, teacher, or school district; aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents; or are otherwise for the use and benefit of the school.” Operators are also prohibited from using this information to amass student profiles, except in furtherance of K-12 school purposes. They also may not sell or rent a student’s information.¹⁶

Operators must implement and maintain reasonable security, delete student information within a reasonable amount of time (unless a student or parent consents to the maintenance of the information), and publicly disclose information about its collection, use, and disclosure of covered information, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.¹⁷

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 3 rd party agreements | Affords quick access to 3 rd 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, and 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, application privacy policies, and district purchases to avoid vulnerabilities | ✓ |
| Align to NIST framework and FERPA policies | Tracks only deidentified aggregated information, and personally identifiable information stays on the district's server; CatchOn has signed the student data privacy pledge | ✓ |
| Privacy training | Enables districts to facilitate training opportunities by leveraging data analytics that track data usage, trends, and impact | ✓ |

¹ 105 ILCS 10/6; see also 23 Ill. Admin. Code § 375.70.

² 105 ILCS 10/6.

³ Illinois State Board of Education. Data Access and Use Policy and Procedures. https://www.isbe.net/Documents/data_access_use_policy.pdf

⁴ 105 ILCS 10/6; 23 Ill. Admin. Code § 375.30.

⁵ 23 Ill. Admin. Code § 375.80(c).

⁶ 23 Ill. Admin. Code § 375.80.

⁷ 105 ILCS 10/4.

⁸ 105 ILCS 10/3.

⁹ 105 ILCS 10/5.

¹⁰ 105 ILCS 10/6.

¹¹ 105 ILCS 10/7.

¹² 105 ILCS 10/9.

¹³ 105 ILCS 13/15.

¹⁴ 105 ILCS 85.

¹⁵ 105 ILCS 85/5.

¹⁶ 105 ILCS 85/10.

¹⁷ 105 ILCS 85/10.

Provided by:



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



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.