Student Data Privacy Policy

District Outreach Industries

Effective Date: May 1, 2026

Last Revised: March 25, 2026

Approved By: Dori Collins, Executive Director

1. Purpose

District Outreach Industries ("DOI," "we," "our," or "us") is committed to protecting the privacy and security of student education records. This policy establishes the standards, procedures, and safeguards that DOI maintains when collecting, using, storing, disclosing, and disposing of student data received from educational agencies and institutions in the course of delivering contracted educational services.

This policy ensures compliance with applicable federal and state student privacy laws, including the Family Educational Rights and Privacy Act (FERPA), the Illinois Student Online Personal Protection Act (SOPPA), and the terms and conditions of data agreements with educational partners.

2. Scope

This policy applies to:

- All DOI employees, contractors, tutors, and volunteers who access, handle, or process student data
- All student information received from schools, school districts, or educational partners
- All systems, platforms, devices, and services used to collect, process, store, or transmit student data
- All third-party service providers and subprocessors that access student data on DOI's behalf

This policy applies regardless of the format of the data (electronic, paper, or verbal) and regardless of whether services are delivered in person or remotely.

3. Regulatory Framework

Authority	Relevance
FERPA (20 U.S.C. §1232g; 34 CFR Part 99)	Federal law protecting the privacy of student education records. Governs access, disclosure, and amendment rights.
SOPPA (105 ILCS 85/)	Illinois Student Online Personal Protection Act. Prohibits targeted advertising using student data, requires data breach notification, limits data collection to educational purposes, and requires operator transparency.
COPPA (15 U.S.C. §6501–6506)	Children's Online Privacy Protection Act. Applies when DOI collects personal information online from children under 13. Schools may provide consent on behalf of parents for educational purposes.

Authority	Relevance
ISSRA (5 ILCS 179/)	Illinois School Student Records Act. State-level protections for student records maintained by Illinois schools.
BIPA (740 ILCS 14/)	Illinois Biometric Information Privacy Act. Applies if DOI collects biometric data (fingerprint, facial recognition). DOI does not currently collect biometric data.
District Data Agreements	Individual data sharing agreements, student data exhibits (e.g., CPS Attachment K), and data processing addenda that impose district-specific requirements.

4. Key Definitions

Term	Definition
Education Records	Records directly related to a student and maintained by an educational agency or institution, or by a party acting on its behalf (34 CFR §99.3).
Personally Identifiable Information (PII)	Information that can be used to identify a student, including name, date of birth, student ID, address, grades, and other direct or indirect identifiers (34 CFR §99.3).
School Official	A contractor or vendor performing institutional services for which a school would otherwise use employees, under the direct control of the school with respect to the use and maintenance of education records (34 CFR §99.31(a)(1)).
Covered Information (SOPPA)	PII or material linked to PII collected by an operator through use of a school's website, service, or application, including educational records, disciplinary records, test results, and other data defined in 105 ILCS 85/5.
Operator (SOPPA)	An entity that operates an internet website, online service, online application, or mobile application with actual knowledge that the site/service is used primarily for K–12 school purposes.
Subprocessor	A third-party service provider engaged by DOI that accesses, processes, or stores student data in connection with DOI's delivery of educational services.
Data Breach	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by DOI.

5. DOI's Role as a School Official

When providing contracted educational services to schools and districts, DOI operates as a "school official" with a legitimate educational interest under FERPA (34 CFR §99.31(a)(1)). In this capacity:

- DOI performs institutional services that the school or district would otherwise use its own employees to provide, including tutoring, academic support, mentoring, and program delivery
- DOI is under the direct control of the educational agency with respect to the use and maintenance of education records
- DOI accesses student information only as necessary to fulfill its contractual responsibilities
- DOI is subject to the same FERPA restrictions on use and redisclosure that govern other school officials

This designation must be established in DOI's agreement with each educational partner. If a district's agreement does not designate DOI as a school official, DOI may not access education records without separate parental consent.

6. Data Collection

A. Data Minimization

DOI collects only the student data that is necessary to perform contracted educational services. Data collection is limited to what is authorized by the educational institution, necessary for service delivery, and permitted under applicable law and the governing data agreement.

B. Categories of Data Collected

The specific data elements collected vary by district agreement. DOI may collect the following categories of student data when authorized and reasonable within the scope of services:

Data Category	Purpose
Student name and identifier	Rostering, tracking, reporting
Email address	Authentication, unique identifier, rostering, notifications (if authorized)
Grade level	Delivery of grade-level-specific content, curriculum matching, rostering, reporting
Classroom and teacher	Curriculum matching, rostering, reporting for school staff
School	Rostering, curriculum matching, reporting
Language	Delivery of services in student's primary language, reporting

Data Category	Purpose
Age / Date of birth	Rostering, age-appropriate content, reporting (date of birth only with authorization)
Student ID	Rostering, reporting
Username and password	Platform authentication (passwords stored in hashed/encrypted form only)
Student grades and test scores	Benchmarking progress, academic matching
Survey responses (non-PII only)	Benchmarking, reporting (cannot be used for marketing per SOPPA)
IP address	Logging, auditing, security
Student-generated content	Storing assessment responses, projects, progress records
Attendance and participation	Program delivery tracking, reporting
Gender	Only when authorized: SEL counseling, college/scholarship matching, bias-free assessment, reporting
Race/Ethnicity	Only when authorized: SEL counseling, college/scholarship matching, bias-free assessment, reporting

DOI does not collect biometric data (fingerprints, facial recognition, voice prints) from students. If a future service requires biometric data, DOI will comply with BIPA (740 ILCS 14/) and obtain all required consents before collection.

C. Methods of Data Collection

Student data is received through:

- Secure file transfer from the educational institution (sFTP, API, or approved web services)
- Integration with the district's approved identity provider and rostering solution
- Direct entry by authorized school personnel into DOI's systems
- Student interaction with DOI's platforms during service delivery

Student data must not be transmitted via email. All data exchange must use secure, encrypted channels approved by the educational partner.

7. Use of Student Data

A. Permitted Uses

DOI uses student information solely to:

- Deliver contracted educational services (tutoring, academic support, mentoring, program delivery)
- Support instruction and monitor student progress
- Communicate with authorized school personnel regarding student performance
- Generate reports required by the educational partner
- Improve the effectiveness of educational services (using de-identified or aggregated data only)

B. Prohibited Uses

DOI does not use student information for:

- Targeted advertising directed at students or their parents/guardians based on student data
- Building a profile of a student for purposes unrelated to educational services
- Marketing or commercial profiling of any kind
- Selling, renting, leasing, or trading student information to any third party
- Any purpose unrelated to the contracted educational services

8. Disclosure of Student Data

DOI does not disclose PII from education records without authorization from the educational institution, except as permitted under FERPA. Permissible disclosures include:

- To authorized school personnel with a legitimate educational interest
- To DOI subprocessors performing services under DOI's direct control, provided they are contractually bound to protect student data, use data only for authorized purposes, comply with FERPA use and redisclosure restrictions (34 CFR §99.33), and are listed in the applicable district data exhibit
- As required by law, court order, or lawfully issued subpoena (with notice to the educational institution where permitted)

DOI does not: sell, rent, lease, or trade student data; disclose student data to third parties not listed in the applicable district data exhibit; or permit unauthorized access to student records.

9. Third-Party Service Providers and Subprocessors

DOI may engage third-party service providers (subprocessors) to support the delivery of educational services. These may include learning platforms, hosting providers, assessment tools, or communication systems.

Requirements for all subprocessors:

1. Must be contractually bound to protect student data consistent with this policy, FERPA, and SOPPA
2. Must use student data only for the purposes authorized under DOI's agreement with the educational institution
3. Must comply with all applicable data protection laws
4. Must be listed in the applicable district data exhibit before accessing student data
5. Must implement security safeguards consistent with or exceeding DOI's own standards
6. Must not further disclose student data without DOI's and the educational institution's authorization

10. Data Security and Safeguards

DOI implements administrative, technical, and physical safeguards to protect student data against unauthorized access, disclosure, alteration, and destruction.

A. Administrative Safeguards

- All DOI personnel who access student data must sign a confidentiality agreement before being granted access
- All personnel receive training on student data privacy, FERPA, and SOPPA requirements upon hire and annually thereafter
- Access to student data is limited to personnel with a legitimate educational need based on their role
- DOI maintains a record of all personnel authorized to access student data

B. Technical Safeguards

- Data encryption in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent)
- Role-based access controls with the principle of least privilege
- Secure authentication systems, including support for district-approved Single Sign-On (SSO) protocols (SAML, OAuth, OpenID Connect, Google SSO, or other approved platforms)
- Unique user accounts for all personnel — no shared credentials
- Regular monitoring and auditing of access logs
- Automatic session timeout for inactive sessions
- Password requirements consistent with industry standards (minimum 12 characters, complexity requirements, 90-day rotation)

C. Physical Safeguards

- Physical access to servers and systems storing student data is restricted to authorized personnel
- Paper records containing student data (if any) are stored in locked cabinets with controlled access
- Devices used to access student data are secured with encryption and remote wipe capability

D. Integration Requirements

When integrating with district systems, DOI will:

- Integrate with the district's approved identity provider and rostering solution
- Support the district's SSO infrastructure
- Exchange data only through secure channels
- Comply with the authentication and integration requirements specified in each district's data agreement

11. Data Breach Notification and Response

In the event of a data breach involving student data, DOI will:

1. Immediately investigate and contain the breach upon discovery
2. Notify the affected educational institution within [24/48/72] hours of confirming the breach, consistent with SOPPA requirements (105 ILCS 85/25) and the applicable data agreement
3. Provide a written report to the educational institution describing the nature of the breach, the data affected, the steps taken to contain and remediate the breach, and recommendations for protecting affected students
4. Cooperate with the educational institution's investigation and notification obligations to parents/guardians
5. Take corrective action to prevent recurrence, including updating security measures, retraining staff, and modifying procedures as needed
6. Maintain documentation of the breach, response actions, and notifications for a minimum of 5 years

12. Data Retention and Destruction

DOI retains student data only as long as necessary to fulfill contractual and educational purposes.

Retention:

- Student data is retained for the duration of the active service agreement with the educational institution
- Upon completion of the contracted service period, data is retained only as required by the terms of the agreement or applicable law
- DOI does not maintain student data indefinitely or beyond the authorized retention period

Destruction:

- Upon request by the educational institution or upon termination/expiration of the service agreement, DOI will securely return or destroy all student data within [30] days
- Electronic data is destroyed using methods consistent with NIST SP 800-88 guidelines (secure deletion, cryptographic erasure, or physical destruction of media)
- Paper records (if any) are destroyed by cross-cut shredding
- DOI provides written confirmation of data destruction to the educational institution upon request
- DOI ensures that subprocessors also return or destroy student data upon termination

13. Parental and Student Rights

Under FERPA, parents (and eligible students age 18 or older) have the right to:

- Inspect and review education records (34 CFR §99.10)
- Request amendment of records they believe are inaccurate, misleading, or in violation of the student's privacy rights (34 CFR §99.20)
- Consent to disclosure of PII from education records, except to the extent FERPA authorizes disclosure without consent

DOI does not respond directly to parent or student requests for access to or amendment of education records unless directed to do so by the educational institution. All such requests should be submitted to the student's school or district. DOI will support the educational institution in fulfilling these requests as required.

14. Illinois SOPPA Compliance

As an operator providing services to Illinois school districts, DOI complies with the Illinois Student Online Personal Protection Act (105 ILCS 85/). DOI's SOPPA obligations include:

- Prohibition on targeted advertising: DOI does not use covered information to engage in targeted advertising directed at students or their parents/guardians
- Prohibition on profiling: DOI does not use covered information to build a profile of a student for purposes other than educational services
- Prohibition on sale of data: DOI does not sell or rent covered information
- Data minimization: DOI collects only the data necessary to provide the contracted educational services
- Data deletion: DOI deletes covered information within a reasonable timeframe upon request by the school or district, or when no longer needed
- Transparency: DOI makes this privacy policy publicly available and responds to district requests for information about its data practices
- Security: DOI implements and maintains reasonable security procedures and practices to protect covered information
- Breach notification: DOI notifies affected school districts in the event of a data breach consistent with SOPPA §25

15. Staff Training and Compliance

DOI maintains internal policies and procedures to ensure compliance with all applicable student data privacy laws:

- All personnel who access student data receive training on FERPA, SOPPA, and DOI's data privacy practices upon hire and annually thereafter
- All personnel sign confidentiality agreements acknowledging their obligation to protect student data
- DOI conducts periodic reviews of its data practices to identify and address gaps
- Violations of this policy by DOI personnel are subject to disciplinary action, up to and including termination and referral to appropriate authorities

16. Roles & Responsibilities

Role	Responsibilities
Data Privacy Officer / Designated Privacy Lead	Oversee compliance with this policy and applicable data privacy laws; manage district data agreements and exhibits; maintain the subprocessor registry; coordinate breach response; conduct staff training; respond to district inquiries about data practices
CEO / Executive Director	Authorize data agreements with educational partners; approve engagement of subprocessors; ensure adequate resources for data privacy compliance

Role	Responsibilities
CFO / Operations Manager	Maintain data security infrastructure; oversee technical safeguards; manage system access and authentication; support breach investigation
Program Staff / Tutors	Handle student data only as necessary to deliver services; follow data handling procedures; report suspected breaches immediately; complete required training

Contact Information:

For questions regarding this policy or DOI's student data practices:

District Outreach Industries

Email: dori@district-outreach.com

Phone: 312-519-2720