



MY SCHOOL IMPROVEMENT PARTNER (MSIP)

DATA PRIVACY AND SECURITY TERMS

Version: 1.0

Version Date: July 14, 2026

These Data Privacy and Security Terms ("Data Terms") govern the collection, access, use, disclosure, storage, processing, retention, protection, and deletion of Client Data in connection with the My School Improvement Partner ("MSIP") platform and are incorporated into each applicable Order Form, SaaS Terms of Service, Statement of Work, and related agreement between WestEd and Client.

1. DEFINITIONS

1.1 Client Data or End User Data

"Client Data" or "End User Data" means all data, records, content, files, information, documents, reports, educational records, student information, and other materials submitted, uploaded, imported, transmitted, generated, or otherwise made available by or on behalf of Client or End User through the Services. "Client Data" or "End User Data" does not include "Outputs."

1.2 Student Data

"Student Data" means any information directly related to a student and maintained by an educational agency or institution, including education records protected by FERPA and any student information protected under applicable state law.

1.3 Personally Identifiable Information (PII)

"Personally Identifiable Information" or "PII" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an identified or identifiable natural person. PII includes, without limitation, an individual's name, address, email address, telephone number, government-issued identification number, Social Security number, driver's license number, passport number, student identification number, employee identification number, financial account information, online identifiers, internet protocol (IP) addresses, geolocation data, biometric information, or any combination of data elements that could reasonably be used to identify a specific individual. For educational institutions, PII also includes "personally identifiable information" as defined under the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g and its implementing regulations.

1.4 Protected Health Information



"Protected Health Information" or "PHI" shall have the meaning assigned to the term "protected health information" under the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations ("HIPAA"), including 45 C.F.R. § 160.103. PHI generally means individually identifiable health information that is transmitted or maintained in any form or medium and relates to an individual's past, present, or future physical or mental health or condition; the provision of healthcare to an individual; or payment for the provision of healthcare to an individual. PHI includes information that identifies, or could reasonably be used to identify, an individual in connection with such health information. PHI does not include information that has been de-identified in accordance with HIPAA requirements.

1.5 Security Incident

"Security Incident" means unauthorized access to, acquisition of, disclosure of, alteration of, loss of, destruction of, or inability to access Client Data or End User Data that compromises the confidentiality, integrity, or availability of such data.

1.6 De-Identified Data

"De-Identified Data" means information that cannot reasonably be used to identify an individual, student, educator, school, district, or Client and that has been stripped of direct and indirect identifiers using industry-accepted methods.

2. CLIENT DATA OWNERSHIP

2.1 Ownership

As between the parties, Client retains all right, title, and interest in and to Client Data.

Nothing in this Agreement transfers ownership of Client Data to WestEd.

2.2 Limited Processing Rights

Client grants WestEd a limited, non-exclusive right to access, process, store, transmit, host, display, and otherwise use Client Data solely to:

- a. provide the Services;
- b. perform Professional Services;
- c. maintain and secure the Services;
- d. comply with legal obligations; and
- e. fulfill obligations under the Agreement.

Client represents that it has all necessary rights, permissions, notices, and authority to provide Client Data to WestEd and authorize WestEd to process such Client Data in accordance with the Agreement.



2.3 No Sale of Data

WestEd shall not sell, rent, trade, disclose, or otherwise monetize Client Data or End User Data.

3. FERPA COMPLIANCE

3.1 School Official Designation

Although Client is expected to avoid uploading student PII, sensitive personal information, and PHI, if Client Data or End User Data inadvertently contains education records protected by FERPA, to the extent Client Data or End User Data includes education records protected by FERPA, the parties acknowledge that WestEd acts as a "school official" with a legitimate educational interest in such records for purposes of performing services on behalf of Client.

3.2 Use Restrictions

WestEd shall use Student Data solely for authorized educational purposes described in the Agreement and shall not use Student Data for targeted advertising, profiling unrelated to educational purposes, or other unauthorized purposes.

3.3 Redisclosure

WestEd shall not redisclose Student Data except:

- a. as authorized by Client;
- b. as required by law; or
- c. to approved Subprocessors subject to written confidentiality and data protection obligations.

3.4 Parent and Student Rights

Client remains responsible for responding to requests from parents, students, guardians, or governmental authorities relating to educational records.

WestEd shall reasonably assist Client in responding to such requests.

4. PRIVACY COMPLIANCE

WestEd shall comply with applicable federal and state privacy laws governing Client Data, including, as applicable:

- FERPA;
- state student privacy laws;
- state breach notification laws;



- applicable consumer privacy laws.

Unless expressly agreed in writing, the Services are not intended for the processing of Protected Health Information subject to HIPAA. The Services may permit Client to upload limited personal information relating to school personnel (such as principal or staff names) where appropriate for the educational purposes of the Services and with an appropriate justification from the Authorized User.

5. INFORMATION SECURITY PROGRAM

5.1 Security Program

WestEd shall maintain a comprehensive written information security program designed to protect the confidentiality, integrity, and availability of Client Data.

5.2 Administrative Safeguards

WestEd shall maintain safeguards including:

- security policies and procedures;
- personnel training;
- confidentiality obligations;
- risk assessments;
- incident response procedures;
- vendor management procedures.

5.3 Technical Safeguards

WestEd shall implement commercially reasonable technical controls including:

- encryption in transit using TLS or equivalent;
- encryption at rest where commercially reasonable;
- role-based access controls;
- multifactor authentication for administrative access;
- logging and monitoring;
- vulnerability management;
- malware protection;
- network security controls.



5.4 Physical Safeguards

WestEd shall utilize commercially reasonable physical safeguards through its facilities and hosting providers.

6. SUBPROCESSORS

As further defined in Addendum 1 of the SaaS Terms of Service, WestEd may engage Subprocessors to support the Services.

WestEd shall:

- a. maintain a current list of Subprocessors;
- b. impose confidentiality and security obligations through written agreements;
- c. remain responsible for Subprocessor compliance with applicable obligations.

Subprocessors may be disclosed through a published Subprocessor Exhibit or upon request.

7. SECURITY INCIDENT RESPONSE

7.1 Incident Response Program

WestEd shall maintain and follow documented procedures for identifying, investigating, containing, mitigating, and remediating Security Incidents.

7.2 Notification

WestEd shall notify Client without unreasonable delay following confirmation of a Security Incident involving Client Data.

To the extent known at the time of notice, WestEd shall provide:

- a. a description of the incident;
- b. categories of affected data;
- c. known impacts;
- d. remediation efforts;
- e. recommended mitigation steps.

7.3 Cooperation

WestEd shall reasonably cooperate with Client regarding investigation, remediation, and legally required notifications.

7.4 No Admission



Notification of a Security Incident shall not constitute an admission of fault or liability.

8. SECURITY AUDITS AND DOCUMENTATION

Upon written request not more than once annually, WestEd shall make available:

- security summaries;
- security program documentation;
- audit reports;
- penetration testing summaries;
- compliance certifications, if available.

WestEd may redact information that would create security risks or disclose confidential security information.

Client shall treat all security documentation as Confidential Information.

9. DATA RETENTION

9.1 Retention During Subscription

WestEd shall retain Client Data or End User Data for the duration of the Subscription Term unless otherwise directed by Client.

9.2 Post-Termination Retention

Following expiration or termination, WestEd may retain Client Data or End User Data for up to ninety (90) days solely for recovery, export, transition assistance, legal compliance, backup restoration, or security purposes.

9.3 Legal Obligations

WestEd may retain data for longer periods if required by law, litigation hold, regulatory obligations, or legitimate business records requirements.

10. DATA EXPORT AND DELETION

10.1 Data Export

Upon Client's written request and subject to the Agreement, WestEd shall make Client Data or End User Data available for export in a commercially reasonable format to the extent WestEd has such Client Data or End User Data retained within the MSIP product.

10.2 Data Deletion



Following expiration of applicable retention periods, WestEd shall securely delete or destroy Client Data or End User Data from production systems, except as otherwise required by law or retained in backup systems.

For the avoidance of doubt, deletion of Client Data, Usage Data, or End User Data does not require deletion of properly de-identified or aggregated information retained pursuant to Section 12.

10.3 Backup Media

Residual copies stored in routine backup systems may remain until overwritten in accordance with standard retention practices.

11. CONFIDENTIALITY

Client Data or End User Data shall be deemed Confidential Information.

WestEd shall protect Client Data or End User Data in accordance with the confidentiality obligations set forth in the Agreement.

Personnel with access to Client Data or End User Data shall be subject to written confidentiality obligations.

12. DE-IDENTIFIED AND AGGREGATED DATA

12.1 Permitted Use

WestEd may create, use, disclose, publish, analyze, and retain De-Identified Data, Usage Data, and aggregated data derived from service usage, operational metrics, feature utilization, system performance, and other deidentified operational information for:

- research;
- analytics;
- benchmarking;
- product improvement;
- service optimization;
- reporting;
- educational research purposes.

CALL Data. Nothing in these Data Privacy and Security Terms limits WestEd's ownership or permitted uses of Survey Data, User Data, or Resulting Data obtained through the CALL platform as authorized under the applicable CALL agreements.

12.2 Prohibited Reidentification

WestEd shall not knowingly attempt to re-identify De-Identified Data.

12.3 No Identification

Any published or disclosed De-Identified Data shall not identify:

- individual students;
- parents;
- educators;
- schools;
- districts;
- Client.

13. AI DATA PROCESSING

13.1 Authorized AI Processing

To the extent the Services include Agentic AI Components, WestEd may process Client Data, including limited personnel information uploaded by Client in accordance with the Agreement, solely to provide AI-enabled functionality authorized under the Agreement.

13.2 No Public Model Training

Unless expressly authorized by Client in writing, WestEd shall not use Client Data or End User Data, Student Data, or educational records to train public-facing or generally available third-party AI models.

13.3 Human Oversight

Client remains responsible for reviewing and validating Outputs before relying upon them for operational, educational, compliance, or policy decisions.

14. CROSS-BORDER DATA TRANSFERS

Unless otherwise agreed in writing, Client Data or End User Data shall be stored and processed within the United States.

If cross-border transfers occur, WestEd shall implement appropriate safeguards consistent with applicable law.

15. RETURN OR DESTRUCTION UPON REQUEST



As further stated in the SasS Terms of Service, upon Client's written request following termination, WestEd shall certify deletion or destruction of Client Data to the extent commercially reasonable and permitted by law and in alignment with WestEd's retention policies and backups.

16. SURVIVAL

The obligations concerning confidentiality, security, data deletion, retained records, audit rights, de-identified data, and Security Incident obligations shall survive termination of the Agreement.

17. ORDER OF PRECEDENCE

In the event of a conflict between these Data Privacy and Security Terms and any other Agreement document, these Data Privacy and Security Terms shall govern with respect to privacy, security, and data protection matters.

END OF DATA PRIVACY AND SECURITY TERMS