Data Privacy Agreement

Sample for review, version 1.1, November 12, 2026.

> **Sample for discussion.** This is a starting point, not legal advice, and it is not binding until both parties sign a final version. Both parties should have it reviewed by their own counsel. Many states and consortia have a standard student data privacy agreement; we are glad to sign yours instead. Bracketed text is to be completed.

1. Parties and purpose

This Data Privacy Agreement ("Agreement") is between [Customer legal name], [address] ("Customer"), and OutcomesPath LLC, 347 5th Ave Ste 1402-405, New York NY 10016 ("Provider"). It applies to the OutcomesPath service the Customer subscribes to (the "Service") and to all Customer Data the Provider receives through it. If this Agreement conflicts with the subscription terms, this Agreement controls for Customer Data.

2. Definitions

"Customer Data" means all information the Customer, its staff, its participants or students, or its partners enter into or upload to the Service, including personally identifiable information, education records, uploaded documents, signed forms, messages and activity logs. "Subprocessor" means a third party the Provider uses to run the Service.

3. Ownership and control

The Customer owns and controls Customer Data. The Provider processes Customer Data only on the Customer's documented instructions and only to provide, secure and support the Service. Where the Customer is an educational institution, the Provider acts as a school official with a legitimate educational interest under FERPA (34 CFR 99.31(a)(1)), under the Customer's direct control for the use and maintenance of education records.

4. Prohibited uses

The Provider will not sell Customer Data; use it for advertising or marketing; build profiles of participants or students other than as the Service requires; use it to train artificial intelligence models; or disclose it except as this Agreement allows or the law requires. If the law requires a disclosure, the Provider will notify the Customer first unless the law forbids it.

5. Provider staff

Provider staff may view Customer Data only to provide support the Customer requested, through read-only access the Customer grants for a set time, or to keep the Service secure and working. Such access is logged and limited to staff bound by confidentiality obligations.

6. Security

The Provider maintains administrative, technical and physical safeguards appropriate to the sensitivity of Customer Data, including: hosting in the United States; encryption in transit and at rest; tenant separation enforced by database row-level security; role-based permissions; multi-factor authentication the Customer can require; session time-outs; an activity log of access and changes; private storage for uploaded documents with time-limited links; daily backups; and monitoring for security events. Safeguards will not be materially reduced during the term.

7. Subprocessors

The Customer authorizes the Subprocessors listed on the Provider's Security page as of the effective date. The Provider binds each Subprocessor to data protection terms no less protective than this Agreement and gives the Customer 30 days' notice before adding a Subprocessor that will handle Customer Data. The Customer may object in writing, and the parties will work in good faith to resolve the objection.

8. Incident notification

The Provider will notify the Customer's designated contact within 72 hours after confirming unauthorized access to or disclosure of Customer Data, or sooner where the law or this Agreement requires, and will provide a written summary of what happened, the data affected, the steps taken and the steps planned. The Provider will cooperate with the Customer's investigation and any notices the Customer must give.

9. Data access and correction

The Customer can export Customer Data at any time in Excel or CSV and can correct or delete records in the Service. The Provider will help the Customer respond to requests from participants, students or parents under applicable law.

10. Retention, return and deletion

Customer Data is retained according to the retention settings the Customer chooses in the Service. On termination, the Customer has 30 days to export Customer Data at no cost, and the Provider will provide a full export on request. After those 30 days the Provider will delete Customer Data from the live Service, and from backups within 30 days after that, except data the law requires to be kept, which remains protected under this Agreement. The Provider will confirm deletion in writing on request.

11. Audit and assurance

On reasonable written request, not more than once a year, the Provider will complete the Customer's security questionnaire and provide current descriptions of its controls and its Subprocessors' security reports where their terms allow.

12. State and sector laws

The Provider will comply with student and consumer privacy laws that apply to the Customer Data, including FERPA, COPPA where participants under 13 are served, and applicable state student data privacy laws. [Add any state-specific terms or the state's standard agreement exhibit here.]

13. Term

This Agreement takes effect on the date of the last signature and continues as long as the Provider holds Customer Data.

14. Governing law

[State] law governs this Agreement. [Customize to match the subscription terms or the Customer's required terms.]

Signatures

Customer	OutcomesPath LLC
Signature:	Signature:
Name:	Name:

Title:	Title:
Date:	Date:

Exhibit A: Customer Data categories

[Check those that apply] Contact information; program enrollment and status; demographics collected for reporting; education records; employment and wage outcomes; uploaded documents (for example IDs, resumes, certificates, signed releases); signed forms; messages; activity logs. [Add others.]

Exhibit B: Customer contacts

Security and incident contact: [name, email, phone]. Privacy contact: [name, email].