K-12 Data Privacy Agreement

Data Privacy and Security Addendum to the One to One Plus Software as a Service Agreement

Version 2026.2

This K-12 Data Privacy Agreement (the "DPA") is between Edutek Solutions, LLC d/b/a One to One Plus ("Provider") and the school system identified in the applicable Order Form ("School System"). It is incorporated into the Software as a Service Agreement and each applicable Order Form. The DPA applies to Provider's processing of School Data in connection with the Services.

1. Scope and Priority

1.1 Scope. This DPA applies whenever Provider receives, maintains, processes, or transmits School Data for the School System in connection with the Services.

1.2 Relationship to Main Agreement and Other Privacy Agreements. Capitalized terms not defined here have the meanings given in the Software as a Service Agreement. If this DPA conflicts with the main Agreement on a privacy or data-security matter, this DPA controls. If the parties sign or otherwise expressly accept a separate state-, consortium-, or School System-required data privacy agreement applicable to the Services, that agreement controls only with respect to privacy and data-security matters and only to the extent it conflicts with this DPA. It does not modify fees, intellectual-property rights, warranties, indemnification, liability limits, governing law, venue, or other commercial terms in the main Agreement unless it expressly identifies the provision being modified and is signed by authorized representatives of both parties.

1.3 Acceptance. Unless applicable law or School System policy requires otherwise, the parties agree that incorporation of this DPA through an accepted Order Form is sufficient. The signature block may be used when a separately executed DPA is required. A School System form, online policy, or state addendum does not bind Provider unless it is incorporated into an Order Form or signed or otherwise expressly accepted in writing by an authorized Provider representative.

2. Definitions

2.1 Applicable Privacy Law. FERPA, PPRA, COPPA to the extent applicable, state student-data privacy and breach-notification laws applicable to the Services and School Data, and other privacy or security laws binding on a party's performance under this DPA.

2.2 Authorized Purpose. Providing, implementing, securing, maintaining, and supporting the Services for the School System as described in the applicable Order Form and Schedule 1.

2.3 Deidentified Data. Data that has been processed so it cannot reasonably identify or be linked to the School System, a student, parent, employee, or other individual, taking into account information reasonably available to Provider.

2.4 School Data. Customer Data that identifies or is reasonably linkable to a student, parent, guardian, applicant, employee, teacher, or other member of the School System community. School Data includes

education records and personally identifiable information from education records as defined by FERPA when applicable.

2.5 Security Incident. Unauthorized acquisition of, access to, use of, disclosure of, alteration of, or destruction of School Data in Provider's possession or control that compromises the confidentiality, integrity, or availability of School Data. Security Incident does not include unsuccessful attempts that do not compromise School Data, such as blocked scans or failed login attempts.

2.6 Subprocessor. A third party engaged by Provider to process School Data in support of the Services.

3. Roles, FERPA Status, and School System Direction

3.1 School System Control. The School System determines the educational and administrative purposes for which School Data is processed, the categories of School Data submitted, Authorized User access, applicable records-retention requirements, and the instructions Provider must follow under this DPA.

3.2 School Official. To the extent FERPA applies, the School System designates Provider as a school official performing institutional services or functions for which the School System would otherwise use employees. Provider will remain under the School System's direct control with respect to the use and maintenance of education records, will use education records only for the Authorized Purpose, and will comply with FERPA's restrictions on use and redisclosure.

3.3 Legitimate Educational Interest. Provider will access education records only to the extent necessary for personnel and Subprocessors to perform the Authorized Purpose and only under access controls established by Provider and the School System.

3.4 School System Responsibilities. The School System is responsible for establishing a lawful basis for disclosing School Data to Provider; providing notices and obtaining consents when required; configuring the Services appropriately; and ensuring that its instructions comply with Applicable Privacy Law.

4. Permitted and Prohibited Uses

4.1 Limited Use. Provider will collect, access, use, maintain, and disclose School Data only for the Authorized Purpose, as directed in writing by the School System, or as required by law.

4.2 No Sale or Advertising. Provider will not sell or rent School Data; use School Data for targeted advertising; build a commercial profile of a student except as necessary to provide the Services; or use School Data to market unrelated products or services to students or parents.

4.3 No Unauthorized Disclosure. Provider will not disclose School Data to a third party except to an authorized Subprocessor, as directed by the School System, or as legally required under Section 11.

4.4 Deidentified Data. To the extent permitted by Applicable Privacy Law, Provider may create and use Deidentified Data for security, analytics, service reliability, benchmarking, and improvement of the Services. Provider will maintain reasonable measures to prevent reidentification, will not attempt to reidentify the data, and will not disclose it in a manner that could reasonably identify the School System or an individual.

4.5 Artificial Intelligence. Provider will not use identifiable School Data to train a general-purpose artificial-intelligence or machine-learning model or a model made available for the benefit of

unaffiliated customers, unless the School System expressly authorizes that use in writing and Applicable Privacy Law permits it. This restriction does not prevent use of the Services, security tools, or customer-specific functionality to process School Data for the Authorized Purpose, or use of Deidentified Data as permitted by Section 4.4.

5. Data Ownership, Transparency, and Minimization

5.1 Ownership. As between the parties, the School System retains all rights in School Data. Provider receives no ownership interest in School Data.

5.2 Data Minimization. Provider will process only School Data reasonably necessary for the Authorized Purpose. The School System will use available configuration and role-based controls to limit data and access to what is reasonably necessary.

5.3 Data Description. Schedule 1 describes the Services, Authorized Purpose, categories of individuals, and anticipated data elements. The parties may update Schedule 1 through an Order Form, implementation record, or other written instruction without otherwise amending this DPA.

5.4 Privacy Information. Provider will maintain publicly available privacy information describing its relevant data practices and will provide additional information reasonably requested by the School System to evaluate the Services.

6. Information Security Program

6.1 Safeguards. Provider will maintain a written information-security program with reasonable and appropriate administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of School Data. The program will be appropriate to the nature of School Data, the Services, and reasonably foreseeable threats.

6.2 Security Measures. Provider's security measures will include the controls summarized in Schedule 2, subject to reasonable updates that do not materially reduce overall protection during an active Subscription Term.

6.3 Personnel. Provider will limit School Data access to personnel who need access for the Authorized Purpose and who are subject to confidentiality obligations and appropriate security and privacy training.

6.4 Independent Assurance. Upon reasonable written request and subject to confidentiality protections, Provider will make available a summary of its then-current independent security assessment or audit report, such as a SOC 2 report, and relevant remediation information appropriate to the School System's review.

6.5 School System Security. The School System is responsible for account administration, role assignment, secure credentials, endpoint security, and timely removal of unauthorized access within systems under its control.

7. Subprocessors

7.1 Use. The School System authorizes Provider to use Subprocessors necessary to provide and support the Services. Provider will conduct reasonable diligence and enter into written terms requiring each

Subprocessor to protect School Data in a manner materially consistent with this DPA and Applicable Privacy Law.

7.2 Responsibility. Provider remains responsible for each Subprocessor's performance of its data-protection obligations to the same extent Provider would be responsible if it performed the processing itself.

8. Security Incident Response

8.1 Notice. Provider will notify the School System without unreasonable delay after determining that a Security Incident affected the School System's School Data and, unless a shorter period is required by Applicable Privacy Law or an agreed state addendum, no later than seventy-two (72) hours after that determination. An initial notice may contain incomplete information and may be updated as the investigation proceeds.

8.2 Information and Cooperation. Provider will take reasonable steps to contain, investigate, mitigate, and remediate the Security Incident and will provide information reasonably available concerning its nature, affected data, timing, corrective actions, and recommended School System steps. Provider will reasonably cooperate with the School System's legally required investigation and response.

8.3 External Notices. The School System controls notices to its students, parents, employees, regulators, and the public unless Applicable Privacy Law requires Provider to provide notice directly. The parties will coordinate the content and timing of notices when legally permitted. Neither party will identify the other publicly as responsible before responsibility has been reasonably established, except as required by law.

8.4 Costs. Provider will bear (a) its own reasonable costs to investigate, contain, mitigate, and remediate a Security Incident and (b) the School System's reasonable, documented third-party costs for legally required notices, mailing, call-center services, and identity-protection or credit-monitoring services, but only to the extent the Security Incident resulted from Provider's or a Subprocessor's breach of this DPA or failure to maintain the safeguards required by it. The School System is responsible for costs to the extent caused by its acts, omissions, configurations, systems, credentials, or instructions. If both parties contributed, costs will be allocated reasonably according to responsibility. Provider is not responsible for optional services or public-relations activities beyond what Applicable Privacy Law requires unless Provider approves them in writing. Amounts payable by Provider under this section are subject to the privacy and security liability cap in Section 14.3 of the main Agreement.

9. Access, Correction, Export, and Requests

9.1 School System Access. During the Subscription Term, the School System may access and correct School Data through available Service functionality. Provider will reasonably assist with access, correction, export, or deletion requests that the School System cannot complete using the Services.

9.2 Individual Requests. If Provider receives a request from a student, parent, eligible student, employee, or other individual concerning School Data, Provider will direct the requester to the School System unless Applicable Privacy Law requires Provider to respond directly. Provider will not independently determine rights in education records on the School System's behalf.

9.3 Record Amendments. Provider will implement corrections or amendments to School Data as directed by the School System, subject to technical feasibility and Applicable Privacy Law.

10. Retention, Return, and Deletion

10.1 During the Term. Provider will retain School Data only as necessary for the Authorized Purpose, the active Subscription Term, documented School System instructions, legitimate security and backup needs, and legal obligations.

10.2 Export. The School System may export available School Data during the Subscription Term using Service functionality. Upon request before expiration or within thirty (30) days afterward, Provider will provide reasonable assistance with a standard export, subject to any professional-services fees disclosed in advance for nonstandard work.

10.3 Deletion. After expiration or termination and completion of any requested export, Provider will delete or render inaccessible School Data from active systems within sixty (60) days, unless a different period is required by law or agreed in writing. School Data in protected backups may remain until overwritten through Provider's ordinary backup cycle, but will remain protected and will not be restored except for disaster recovery or legal necessity.

10.4 Legal Retention. If Provider must retain specific School Data by law, Provider will isolate and protect it, use it only for the legal obligation, and delete it when retention is no longer required.

10.5 Certification. Upon reasonable written request, Provider will confirm completion of deletion consistent with this section.

11. Legal Demands and Government Requests

11.1 If Provider receives a subpoena, court order, public-authority demand, or other legal request for School Data, Provider will, to the extent legally permitted, promptly notify the School System and provide reasonable cooperation so the School System may seek protection. Provider will disclose only the School Data legally required and will direct the requesting party to the School System when appropriate.

12. Compliance Reviews

12.1 Documentation. Provider will respond reasonably to a School System security or privacy questionnaire and provide available compliance documentation no more than once annually, unless a Security Incident or material legal requirement justifies an additional review.

12.2 Audits. If documentation is not reasonably sufficient to demonstrate compliance with a material legal requirement, the parties will agree on a proportionate review that protects other customers, Provider security, and confidential information

13. Children's Privacy

13.1 To the extent COPPA applies to the Services, Provider will comply with applicable operator obligations and will use personal information collected from children only for the educational service requested by the School System and other purposes permitted by law. Where the School System may

provide consent on behalf of parents under COPPA, Provider will give the School System the notices and information reasonably necessary for that decision. Nothing in this DPA transfers Provider's independent legal obligations to the School System.

14. Data Location and Transfers

14.1 United States Hosting. Provider will host production School Data and backups in the United States. Provider will not relocate the primary hosting environment outside the United States or permit routine processing of identifiable School Data outside the United States without prior written notice, legally appropriate safeguards, and School System approval when Applicable Privacy Law requires it.

15. Change of Control and Assignment

15.1 Provider may transfer School Data to a permitted successor or assignee under the main Agreement only as necessary to continue the Services and only if the successor remains bound by this DPA. A merger, financing, equity sale, reorganization, or sale of the business does not authorize any new use of School Data. Provider will provide notice of a material change in ownership when required by Applicable Privacy Law or an agreed state-specific addendum.

16. Liability, Term, and Survival

16.1 Liability. The limitations, exclusions, remedies, and allocation of risk in the main Agreement apply to this DPA unless Applicable Privacy Law prohibits their application. Costs allocated to Provider under Section 8.4 count toward the separate privacy and security cap in Section 14.3 of the main Agreement.

16.2 Term. This DPA begins when it is incorporated into an accepted Order Form or separately signed and continues while Provider processes School Data for the School System.

16.3 Survival. Provider's restrictions on use and disclosure and its obligations concerning security, incident cooperation, and data disposition survive for as long as Provider retains School Data.

17. State-Specific Requirements

17.1 Required Privacy Agreements. The parties may attach or incorporate a state-specific privacy rider, Student Data Privacy Consortium agreement, National Data Privacy Agreement exhibit, or other legally required privacy terms. A separate privacy agreement signed or otherwise expressly accepted by both parties controls only as stated in Section 1.2. If the School System requires its own privacy agreement, the parties may use that agreement instead of Provider's standard DPA for conflicting privacy and data-security matters while leaving the commercial provisions of the main Agreement in effect.

17.3 State-Law Compliance. The parties acknowledge that certain jurisdictions impose contract terms, security standards, breach timelines, parent-notice materials, or data-destruction requirements beyond this general DPA. Provider will use the mutually executed School System privacy agreement rather than representing that this general DPA alone satisfies every jurisdiction.

Schedule 1 - Processing Details

Item	Description
Services	One to One Plus hosted K-12 asset-management, help-desk, implementation, support, reporting, mobile, integration, and related services purchased in the Order Form.
Authorized Purpose	To provide the purchased Services for the School System's K-12 administrative and operational functions, including asset assignment and lifecycle management, help-desk ticketing, user and location administration, reporting, support, and configured integrations.
Data subjects	Students, parents or guardians where configured, employees, teachers, contractors, and other Authorized Users.
Processing duration	The applicable Subscription Term plus the limited export, backup, and legal-retention.

Anticipated Data Categories

Category	Examples	Scope note
Identity and directory	Name, district or student identifier, username, school email, role, grade level where configured	Only fields enabled and supplied by the School System
School organization	School, department, classroom, location, graduation year, enrollment or employment status	As configured
Asset management	Device or asset identifiers, assignments, checkout and return records, condition, warranty, repair, loss, fee, and inventory history	Core asset-management functions
Help desk	Ticket content, category, priority, requester, assignee, timestamps, status, notes, and attachments	School System should avoid unnecessary sensitive data in free-text fields
Technical and usage	IP address, device/browser details, authentication and audit events, logs, feature usage, and diagnostic information	Security, support, and service operation
Integration data	Identifiers and records exchanged through School System-authorized SIS, directory, device-management, SSO, payment, or other integrations	Limited to configured integrations

Schedule 2 - Baseline Security Measures

Provider's security and operations teams must confirm each statement before customer use. Controls may be updated if the overall level of protection is not materially reduced.

Control area	Baseline measure
Governance	Written information-security policies, assigned security responsibility, risk assessment, incident-response procedures, and periodic control review.
Independent assurance	SOC 2 Type 2 examination or comparable independent assessment, with appropriate summary information available under confidentiality protections.
Hosting	Cloud hosting using Amazon Web Services (AWS) in the United States.
Access control	Role-based and least-privilege access, unique accounts, controlled privileged access, authentication safeguards, and prompt access removal.
Logging and monitoring	Security and administrative logging appropriate to the Services, monitoring of relevant events, and procedures for investigation and escalation.
Secure development	Change control, code review and testing practices, dependency and vulnerability management, and remediation based on risk.
Resilience	Backups, recovery procedures, availability monitoring, and periodic testing appropriate to the Services.
Personnel	Confidentiality obligations and security and privacy awareness training for personnel with relevant access.
Vendor management	Risk-based review of Subprocessors and written data-protection obligations.
Data disposal	Secure deletion or rendering inaccessible in accordance with documented retention and disposal procedures.

Schedule 3 - Subprocessor Information

Maintain the current production list at a permanent URL and ensure it matches actual data flows before publication.

Subprocessor	Purpose	Processing location
Amazon Web Services, Inc.	Cloud infrastructure and hosting	United States

Signatures

EDUTEK SOLUTIONS, LLC

Entity Name: Edutek Solutions, LLC

Signature:
_____

Name:
_____

Date:
_____

CUSTOMER

Entity Name:
_____

Signature:
_____

Name:
_____

Date:
_____