NEW YORK PACKAGE

SpecialNeedsWare, Inc. dba Ori Learning · Version v2026.09 · Effective September 23, 2026

How this package is used

This package is the State Addendum for New York under Section 16.4 of the Data Privacy Addendum. It has three parts: **Part A**, the contract-specific supplement to the educational agency's Parents' Bill of Rights for Data Privacy and Security (8 NYCRR §121.3(c)); **Part B**, Ori Learning's Data Security and Privacy Plan for the agency's acceptance (§121.6); and **Part C**, an Education Law §2-d and Part 121 addendum used only where the agency has no data privacy agreement of its own. Parts A and B are completed for each agency and each Order Form and attach to whatever instrument the agency uses: its own agreement, the New York State Education Department's model data privacy agreement, a Regional Information Center or BOCES agreement, a National Data Privacy Agreement with the New York supplement, or, where the agency has none, Part C. A signed copy of the agency's Parents' Bill of Rights, and the agency's data security and privacy policy adopted under §121.5 (its title, its date and the date it was provided), are attached to Part B (Education Law §2-d(5)(e); Part B heading). **One formation trigger.** Parts A and B take effect, and the agency's acceptance of Part B under §121.6 is given, when the agency accepts the instrument that incorporates them, whether the Order Form or the agency's own instrument to which they attach, or signs them where the agency requires a signature (B.8); Part C takes effect as C.11 states. Ori Learning receives no student data from the agency before that instrument has been accepted and the privacy instrument the agency uses is in place, on the gate Data Privacy Addendum §1.6 states and the Order Form records, and before the agency's §121.5 policy has been provided. **Ladder position.** This package sits at rung (b) of the order of precedence (C.2). Where Parts A and B attach to an instrument the agency brings, that instrument sits at rung (a) as to the treatment of Student Data and varies Sections 11 to 14 of the Master Subscription Agreement only where it names the term (Data Privacy Addendum §1.3), and a section of the Data Privacy Addendum this package cites that the agency's instrument displaces is read as the equivalent provision of that instrument. **Versions.** The version of this package identified on the Order Form, or accepted by the agency, governs for the Subscription Term; a re-issued version is provided for information and binds the agency only as Master §15.3 provides, at renewal or by a written amendment signed by both parties, and the same applies to a re-issued Security & Incident Exhibit, subject to the improvement rule in Data Privacy Addendum §15.3. Capitalized terms in every Part have the meanings given in the Ori Learning Definitions, published at orilearning.com/legal/definitions/; the Information Security Program, the Incident Response Plan, the Data Retention & Deletion Policy and the Business Continuity and Disaster Recovery Plan are Ori Learning's internal documents so titled, described in the Security & Incident Exhibit. In Parts A and B, a section cited as "§" followed by a number alone is a section of the Data Privacy Addendum, and one cited as "§121." followed by a number is a section of 8 NYCRR Part 121.

Part A — Parents' Bill of Rights for Data Privacy and Security: Contract-Specific Supplement (8 NYCRR §121.3(c))

Educational agency: Educational agency name · **Contractor:** SpecialNeedsWare, Inc. dba Ori Learning, 66 Summit Ave, Chatham, NJ 07928 · **Agreement:** Each operative instrument executed for the agency, by title, version and date · **Products and Sites:** Products and Sites from the Order Form · **Contract term:** Subscription Term start date to Subscription Term end date · **Agency Data Protection Officer:** Name, title and email of the agency's Data Protection Officer

§121.3(c) element	Supplemental information for this Agreement
(1) The exclusive purposes for which the student data will be used	To provide the Products to the agency and its Authorized Users for the School-Authorized Educational Purpose and for no other purpose: creating and administering Accounts, organizations, Sites, classes and rosters; delivering the Curriculum Content the agency assigns, including assessments, check-ins and, where the agency enables them, class-visible Collaboration Boards; recording Students' responses, work, progress and results and reporting them to the Student and to the agency's Teachers and Administrators; adapting instruction where a Product provides it; supporting and training the agency's users and communicating with them about the Services, including through the customer-success platform the Subprocessor Schedule lists; operating, maintaining, securing and repairing the Platform, including the product-usage analytics that report to the agency; and complying with law and the Agreement (Data Privacy Addendum §5.2(a)–(i)). A further purpose the agency directs in writing under Data Privacy Addendum §5.2(j) applies to the agency's data only once this supplement is amended to state it. Ori Learning does not sell student data, use it for advertising, marketing or any commercial purpose, use it to develop or improve products or services except as De-identified Data or Aggregate Data, or use it to train any artificial-intelligence model, and does not authorize any Subprocessor to use it to train one (§5.3–5.5).

§121.3(c) element	Supplemental information for this Agreement
(2) How subcontractors and other authorized recipients will comply with the applicable data protection and security requirements	Ori Learning uses the subcontractors, which the Ori Learning Definitions call Subprocessors, that the Subprocessor Schedule at orilearning.com/legal/subprocessors/ lists, which is part of the Agreement and states each one's legal entity, function, the data it receives, whether it receives student data, its processing location and its terms: Microsoft Corporation (Microsoft Azure hosting of the Platform and every production data store, Azure Application Insights logging, and Azure SignalR real-time transport; United States); Google LLC (Cloud Translation and Cloud Text-to-Speech for lesson text, and Cloud Translation for any Student-written text the Platform sends for translation); Amplitude, Inc. (product-usage analytics that report to the agency; student usage events under a pseudonymous identifier, never a Student's name, username or contact details); ChurnZero, Inc. (customer-success platform; student usage events under a pseudonymous identifier, never a Student's name, username or contact details, and staff usage events; United States); TrackJS, LLC (Request Metrics error and performance monitoring; United States); Twilio Inc. (SendGrid transactional email; a Student's email address where the agency supplies one; United States); and HubSpot, Inc. (educator support chat and customer relationship management; no student data in the sync). Before a Subprocessor receives student data, Ori Learning evaluates its ability to protect the data and ensures that its written terms, which may be its standard published data-protection terms, require it to protect student data consistent with the Data Privacy Addendum, and limit its use to providing its services to Ori Learning; Ori Learning does not authorize any Subprocessor to use student data to train an artificial-intelligence model (Data Privacy Addendum §9.2). Where Ori Learning engages a Subprocessor to perform its obligations under the Agreement, the data protection obligations that state and federal law and the Agreement impose on Ori Learning apply to that Subprocessor (8 NYCRR §121.9(b)). Ori Learning remains responsible for each Subprocessor as if for itself. Ori Learning keeps the Subprocessor Schedule current and notifies the agency's privacy and security contact by email of changes to it, and an agency that objects to a change on reasonable grounds relating to the protection of student data may terminate the affected Services and receive a refund of prepaid Fees for the remainder of the Subscription Term (§9.6); a material change to the collection, use or disclosure of student data requires the agency's renewed authorization (Data Privacy Addendum §15.4). Platform pages load fonts and similar resources from the providers listed on the Subprocessor Schedule, which receive the network information a browser sends with any web request; Ori Learning evaluates each such service and uses it only in compliance with Applicable Law and the Data Privacy Addendum. Development of the Platform is performed in the United States under the direction of Ori Learning's Chief Technology Officer, and no one other than the Chief Technology Officer develops the Platform; support is provided by Ori Learning Personnel under the access controls the Security & Incident Exhibit describes (§9.8; Security & Incident Exhibit §3.3).
(3) The duration of the contract, and what happens to the student data upon expiration, including whether, when, how and in what format the data will be returned or destroyed	Duration: the contract term stated above, and any renewal on a new Order Form. On expiration or termination the agency may export its data during the 60 days after the Services end, with Ori Learning's assistance, and receives a machine-readable copy on request (Data Privacy Addendum §12.3); at the agency's written direction, and as this package rather than the Data Privacy Addendum provides, Ori Learning delivers that export to a successor provider the agency designates. Ori Learning then Deletes the agency's student data within 30 days after the earlier of the agency's written confirmation that its export is complete and the end of those 60 days, and in any case no later than 90 days after the Services end, unless the agency renews, directs earlier Deletion, gives a written transition instruction as §12.4 provides, or a Legal Hold applies (§12.4). Deletion renders the data no longer accessible or recoverable through the Platform and instructs each Subprocessor to delete it; disaster-recovery Backups, which Azure states it encrypts at rest, are inaccessible for ordinary use, are never used to restore Deleted data except to recover the Platform as a whole (after which the Deletion is re-applied), and age out on their rotation (§12.5). Ori Learning gives the agency a written certification stating what was Deleted, the method and the date, without request after the end-of-term Deletion and on request after any other (§12.6).

§121.3(c) element	Supplemental information for this Agreement
(4) If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data	A parent, student or eligible student challenges the accuracy of student data through the educational agency under its procedures for amending education records under FERPA and Education Law §2-d; requests are not made to Ori Learning, and a request that reaches Ori Learning is acknowledged within 5 Business Days and referred to the agency's privacy and security contact identified under Data Privacy Addendum §17.3, which for the agency is its Data Protection Officer unless the agency names another (Data Privacy Addendum §7.3). The agency corrects roster and Account data through its Administrator tools and directs Ori Learning to correct or annotate other student data, which Ori Learning does within 30 days after the direction and confirms in writing (§7.4, §7.6); the agency's 45-day period for inspection and review under §121.12 is supported as Part C, C.9 states. Teachers and principals: a challenge to the accuracy of annual professional performance review data is made to the agency under §121.12.
(5) Where the student data will be stored, described in a manner that does not create a security risk, and the security protections taken to ensure it will be protected, including whether it will be encrypted	Student data in the Platform is stored at rest in Microsoft Azure data centers in the United States (Data Privacy Addendum §10.2(g)); each Subprocessor's processing location is as the Subprocessor Schedule describes it. It is protected by the written Information Security Program described in the Security & Incident Exhibit, which states which controls are In place and which are Adopted, with the milestone by which each Adopted control takes effect, and summarized in Part B: role-based access limited to the agency's organization, Sites and classes; individually authenticated Personnel access on a need-to-know basis; encryption in transit and at rest (element 6); logging and monitoring; vulnerability and patch management; an Incident Response Plan; training and confidentiality agreements completed before any person accesses the agency's data (B.4); and, Adopted with effect from the milestones the Security & Incident Exhibit states, an annual risk assessment (§10.2(f)), an annual independent penetration test (Security & Incident Exhibit §3.3–3.4) and Personnel screening (§10.2(c)). The parts of the Security & Incident Exhibit that are security-sensitive are identified so that the agency may redact them when it publishes this supplement (§121.3(e); Data Privacy Addendum §13.6).
(6) How the student data will be protected using encryption while in motion and at rest	In motion: every connection to the Platform is encrypted in transit using HTTPS, and each Subprocessor is engaged under terms that require it to protect student data (Data Privacy Addendum §9.2). At rest: every production data store that holds the agency's student data, including the SQL database and file (Blob) storage, is encrypted at rest by Azure platform encryption, and Azure states that it encrypts database Backups at rest; as an additional control, and not as the standard §121.9(a)(7) requires, name, username, email address, telephone number and external identifier fields are encrypted at the field level before they are written to the database, with keys held in a managed key vault separate from the data. The transport-layer encryption and the Azure platform encryption described above are technologies within the guidance the Secretary of Health and Human Services issued under Section 13402(h)(2) of Public Law 111-5 (8 NYCRR §121.1(i)).

Ori Learning supplied the information above. **For the educational agency:** the agency adopts this supplement as its contract-specific supplement under 8 NYCRR §121.3(c) by accepting Part B (B.8) or by completing the block below. Agency: Educational agency name · By: Name and title · Date: Date · **For Ori Learning:** Jonathan Izak, Chief Executive Officer · Date: Date

Part B — Data Security and Privacy Plan (8 NYCRR §121.6)

Contractor: SpecialNeedsWare, Inc. dba Ori Learning · **Educational agency:** Educational agency name · **Agreement:** Each operative instrument executed for the agency, by title, version and date · **Agency Data Security and Privacy Policy (required):** Title and date of the agency's policy under §121.5, provided to Ori Learning on Date provided · **Plan version:** v2026.09, effective September 23, 2026 · **Attachment:** a signed copy of the agency's Parents' Bill of Rights

Where the agency has not yet provided its §121.5 policy, Part C, C.3 attaches to the policy as and when it is provided, and this Plan is not effective for the agency until it has been provided.

This Plan describes how Ori Learning protects the personally identifiable information it receives from the educational agency under the Agreement, over the life of the Agreement. It describes as in place only safeguards that are in place when Ori Learning receives the agency's student data; a safeguard Ori Learning has adopted but not yet put in place is not described as in place, and its milestone is stated in the Security & Incident Exhibit (B.2). Ori Learning holds no SOC 2 report, no ISO/IEC 27001 certification and no third-party penetration-test report and claims none; its Accessibility Conformance Report (VPAT) and its HECVAT-Lite questionnaire are self-authored and self-evaluated and are not a certification, attestation or audit. The version of this Plan the agency accepts governs for the Subscription Term. Ori Learning re-issues the Plan at each renewal and on any material change to the data, purposes, storage, Subprocessors or data lifecycle it describes; a re-issued Plan is provided for information and binds the agency only when accepted under B.8 or as Master §15.3 provides.

B.1 Implementation of the applicable requirements (§121.6(a)(1)). Ori Learning implements the requirements of Education Law §2-d, 8 NYCRR Part 121, federal law (FERPA, COPPA and IDEA Part B as they apply, and the Protection of Pupil Rights Amendment where it applies to the agency), the Agreement and the agency's Data Security and Privacy Policy identified above, throughout the life of the Agreement, through a written Information Security Program maintained under 16 C.F.R. §312.8 and described in the Security & Incident Exhibit. Its Chief Technology Officer, by role, is its Security Officer, coordinates the program and leads the response to Security Incidents; its Privacy Officer, by role, is Ori Learning's designated privacy official and the official responsible for the confidentiality of personally identifiable information under IDEA Part B, reached at legal@orilearning.com, which Ori Learning reads on Business Days; its Chief Executive Officer is accountable for the program. Ori Learning evaluates the program at least once a year, after any material change to the Platform or its Subprocessors, after any significant incident, and on any change in the law that applies to the agency, and the Security & Incident Exhibit is re-issued at each evaluation. Ori Learning obtains the agency's §121.5 policy at contracting and applies it to the agency's student data (C.3); the terms Education Law §2-d and Part 121 require of a third-party contractor are carried in this package (Part C) or in the agency's own instrument. Ori Learning designs the Curriculum Content not to ask students to reveal information in the categories listed in 20 U.S.C. §1232h(b); an agency that believes an item does may ask Ori Learning to review it, and at the agency's direction Ori Learning removes the item from the agency's assignments (Data Privacy Addendum §8.3). Ori Learning answers the agency's reasonable privacy and security questionnaire before the Agreement begins and once a year after (§13.2), and cooperates with the Chief Privacy Officer under §121.11.

B.2 Administrative, operational and technical safeguards (§121.6(a)(2)). Ori Learning aligns its technologies, safeguards and practices with the NIST Cybersecurity Framework 2.0 (§121.9(a)(1)) and organizes its program by the framework's six functions; the alignment is Ori Learning's own assessment, summarized for the agency on request, and is not a certification, and the framework is a reference, not a mapping or a conformance claim (Security & Incident Exhibit §3.2). This Plan states the safeguards at category level. The Security & Incident Exhibit, provided to the agency under the confidentiality terms of the Agreement, carries the control-by-control statement, the status of each control and the milestones for Adopted controls, and is the operative source for every control this table summarizes. Every safeguard this table describes is in place when Ori Learning receives the agency's student data, except that a safeguard the Exhibit marks Adopted takes effect by its milestone (C.5).

Function	Safeguards
Govern	The written Information Security Program, Incident Response Plan and Data Retention & Deletion Policy, adopted by the Chief Executive Officer and evaluated at least annually; a risk assessment, first performed on the milestone the Security & Incident Exhibit states and repeated at least annually and before any material change; a truthfulness rule under which no document or questionnaire answer describes a control the program does not record.
Identify	An inventory of systems, data stores, Subprocessors and Personnel access; the public Subprocessor Schedule; a data inventory by role (Data Privacy Addendum Annex A); classification of the agency's data as student data protected under Education Law §2-d; evaluation of each Subprocessor before it receives student data, and the written terms Data Privacy Addendum §9.2 describes; evaluation of each service Platform pages load.
Protect	Role-based access limited to the agency's organization, Sites and classes; individually authenticated Personnel access on a need-to-know basis; passwords stored only as hashes; short-lived access tokens; encryption in transit and at rest, with field-level encryption of specified personal fields and keys in a managed key vault as an additional control (Part A, element 6); secure development practices; Personnel confidentiality agreements signed and training completed before access, the training repeated annually (B.4); endpoint protection, monitoring and patching through a managed information-technology and security provider; hosting on Microsoft Azure in the United States, with Microsoft's physical security.
Detect	Application and activity logging; monitoring and alerting through the managed provider; vulnerability scanning and independent testing on the cadences the Security & Incident Exhibit states, with summaries available to the agency under confidentiality; administrative-action logging and review of security logs at least monthly, from the milestone the Security & Incident Exhibit states.
Respond	The Incident Response Plan (B.6): detection, classification, containment, investigation, notice to the agency and cooperation with it and with law enforcement; preservation of evidence; a factual post-incident review when the investigation is reasonably complete; an annual tabletop exercise.
Recover	Azure Backups on a limited rotation, which Azure states it encrypts, kept in the United States; a business continuity and disaster recovery plan, with recovery objectives and a restoration test on the milestones the Security & Incident Exhibit states; Backups used only to recover the Platform as a whole, with any Deletion re-applied after a restore.

Status. The Security & Incident Exhibit §3.3 carries the status of each control. Safeguards the Exhibit marks Adopted, among them the annual independent penetration test, the production access register, the separated-environments rule, administrative-action logging, and the recovery objectives and restoration test, are commitments with milestone dates and are not part of this Plan's description of present safeguards.

B.3 Compliance with the Parents' Bill of Rights supplement (§121.6(a)(3)). Ori Learning complies with each element of Part A as follows: element 1 through the purpose limitation and prohibited uses in Data Privacy Addendum §5, enforced by role-based access, by the Subprocessor terms B.5 describes,

which limit each Subprocessor's use of student data to providing its services to Ori Learning, and by Ori Learning's authorizing no Subprocessor to train an artificial-intelligence model on student data; element 2 through the Subprocessor terms and change notice in B.5; element 3 through the export, Deletion and certification process in B.7; element 4 through the request routing and correction process in Data Privacy Addendum §7 and Ori Learning's request register; element 5 through the safeguards in B.2 and the United States hosting the Security & Incident Exhibit describes; and element 6 through the encryption controls in B.2 and Part A, element 6.

B.4 Training before access (§121.6(a)(4)). Before any officer or employee of Ori Learning or of its assignees is given access to the agency's student data, that person completes training on the federal and state laws governing the confidentiality of student data and teacher and principal data, covering FERPA, COPPA, IDEA Part B, Education Law §2-d and Part 121, role-based access, the uses and disclosures the Agreement authorizes, the prohibition on commercial and marketing use, the agency's policy, and incident escalation, together with Ori Learning's Information Security Program, Incident Response Plan and Data Retention & Deletion Policy; completion is recorded and the record is available to the agency on request. Ori Learning repeats the training at least once a year. Each such person signs a confidentiality agreement before access. Training and the confidentiality agreement are conditions of access, not commitments with a grace period, and every person who holds access when this Plan is accepted has completed both. Screening of Personnel before access to student data is the screening the Security & Incident Exhibit states, on its milestone. For a subcontractor's personnel, the data protection obligations that apply to Ori Learning apply to the subcontractor (§121.9(b)).

B.5 Subcontractors (§121.6(a)(5)). Ori Learning uses the subcontractors Part A, element 2, identifies. It manages them as follows: before a subcontractor receives student data, Ori Learning evaluates its ability to protect the data and ensures that its written terms, which may be its standard published data-protection terms, require it to protect student data consistent with the Data Privacy Addendum, and limit its use to providing its services to Ori Learning, and it takes reasonable steps to use only subcontractors capable of maintaining the confidentiality, security and integrity of student data (Data Privacy Addendum §9.2; 16 C.F.R. §312.8); the data protection obligations that state and federal law and the Agreement impose on Ori Learning apply to each subcontractor that performs Ori Learning's obligations under the Agreement (§121.9(b)); and Ori Learning remains responsible for each subcontractor as if for itself (§9.4). Ori Learning keeps the Subprocessor Schedule current and notifies the agency by email of changes to it, and an agency that objects to a change on reasonable grounds relating to the protection of student data may terminate the affected Services (§9.6); Ori Learning ends a subcontractor's access on a material breach (§9.5). No one other than the Chief Technology Officer develops the Platform; a development subcontractor later engaged would be listed on the Subprocessor Schedule before it received any data.

B.6 Incident identification, management and notice to the agency (§121.6(a)(6)). Ori Learning identifies incidents through its managed security provider's monitoring and alerts, Platform and application logs, administrative-action logs from the milestone the Security & Incident Exhibit states, Personnel reports, reports from the agency and its users to support@orilearning.com or legal@orilearning.com, and Subprocessor notices; its Personnel must report a suspected incident at once. Each incident is recorded, classified by severity, contained, investigated and remediated under the Incident Response Plan, with an incident preservation hold on the evidence from discovery. Ori Learning notifies the

agency of any breach or unauthorized release of its personally identifiable information, including any event in which that information was accessible to an unauthorized person, in the most expedient way possible and without unreasonable delay, and no later than seven calendar days after discovery (§121.10(a)); that period runs from discovery, independently of when Ori Learning confirms an Unauthorized Release under the Data Privacy Addendum and of any delay a law-enforcement direction permits for other notices. The notice the Data Privacy Addendum requires, given without unreasonable delay and no later than 72 hours after Ori Learning confirms an Unauthorized Release (Data Privacy Addendum §11), may satisfy the seven-day notice where its timing and content suffice. Each notice is clear and plain and states, to the extent available, the dates of the incident and of its discovery, a description of the incident, the types of personally identifiable information affected, the estimated number of records affected, the investigation or the plan for it, and a contact (§121.10(g)), so that the agency can report to the Chief Privacy Officer within ten calendar days (§121.10(b)) and notify parents, eligible students, teachers and principals (§121.10(e)). Ori Learning cooperates with the agency and with law enforcement to protect the integrity of the investigation (§121.10(c)), preserves logs and evidence, updates the agency as material facts become known and, on the agency's request after the incident is resolved, gives it a written summary of the incident's cause and the remediation performed (Data Privacy Addendum §11.5), and pays for or promptly reimburses the agency for the full cost of the notifications §121.10 requires the agency to give where the incident is attributed to Ori Learning or a Subprocessor (§121.10(f); Part C, C.7). The Incident Lead (the role the Security & Incident Exhibit §4.1 describes) issues each notice; the Chief Executive Officer reviews it where practicable, the Deputy the Security & Incident Exhibit §4.1 names acts where neither is available, and no internal approval delays a notice this Section requires.

B.7 Return, transition, deletion or destruction on expiration or termination (§121.6(a)(7)). The Export Window, the machine-readable copy on request, the transition of the export to a successor provider at the agency's written direction, the Deletion periods and the Backup treatment are stated in Part A, element 3, which rests on Data Privacy Addendum §12.3–12.5 for every limb except the transition to a successor, a term of this package alone. Operationally: Deletion removes the data from Ori Learning's active systems so that it is no longer accessible or recoverable through the Platform, cascading to assignments, activity, progress and session records, and instructs each Subprocessor to do the same; NIST Special Publication 800-88 is guidance for the method; the exceptions are those Part A, element 3, states (renewal, the agency's direction to Delete earlier, a written transition instruction and a Legal Hold) and a statutory preservation duty, and data held under any of them is used for no other purpose. Ori Learning's written certification (§12.6) states the scope, the date and method of each Deletion, the Subprocessors instructed and their confirmations, that Backups age out on their rotation, and any Legal Hold exception.

B.8 Acceptance. This Plan forms part of the Agreement and is accepted by the educational agency as the contractor's Data Security and Privacy Plan under §121.6 when the agency accepts the instrument that incorporates it, or signs below where it requires a signature; the agency's acceptance also adopts Part A as its contract-specific supplement.

For the educational agency	For Ori Learning
Name: Name	Name: Jonathan Izak
Title: Title	Title: Chief Executive Officer
Date: Date	Date: Date
Signature: Signature	Signature: Signature

Part C — Education Law §2-d and Part 121 Addendum

Used only where the educational agency has no data privacy agreement of its own.

C.1 When this Addendum applies. This Addendum applies where the Customer is an educational agency within the meaning of Education Law §2-d and 8 NYCRR §121.1, including a school district, a board of cooperative educational services, a charter school and an approved private school for the education of students with disabilities, and has not executed with Ori Learning a data privacy agreement of its own, the New York State Education Department's model data privacy agreement, a Regional Information Center or BOCES agreement, or a National Data Privacy Agreement with the New York supplement. Where the Customer has executed one of those instruments, that instrument, with Parts A and B, is the parties' arrangement under §2-d, and this Addendum does not apply.

C.2 A State Addendum; order of precedence. This Addendum, Part A and Part B together are the New York package, the State Addendum for New York under Section 16.4 of the Data Privacy Addendum, executed for the Customer when the Customer accepts the instrument that incorporates it or signs it (B.8 for Parts A and B; C.11 for this Addendum). Capitalized terms have the meanings given in the Ori Learning Definitions; "personally identifiable information", "student data", "educational agency", "third-party contractor", "breach" and "unauthorized release" have the meanings given in Education Law §2-d and 8 NYCRR §121.1, and personally identifiable information from student records that Ori Learning receives from the Customer is Student Data.

> **Order of precedence.** If the documents that make up the Agreement conflict, the document listed higher below controls to the extent of the conflict:
>
> (a) a Data Privacy Agreement executed by both the Customer and Ori Learning, including a National Data Privacy Agreement, a state form, or a Customer-authored agreement, as to the treatment of Student Data, and as to a term of Section 11, 12, 13 or 14 of the Master Subscription Agreement only where it names the term it varies;
>
> (b) a State Addendum executed for the Customer, as to its subject matter;
>
> (c) the Data Privacy Addendum, including its Exhibits and Annexes, as to Student Data and Customer Data;
>
> (d) the Order Form, with its Schedule 1 and any award-specific addendum attached under it, except that a term the award-specific addendum identifies as one the federal award or cooperative contract makes mandatory controls a conflicting term of any document listed here to the extent the law requires and no further;
>
> (e) the Master Subscription Agreement;
>
> (f) the Accessibility Exhibit and the Acceptable Use Policy, in that order; and
>
> (g) the Authorized User Terms and any posted notice or policy, which bind only the individual who accepts them, whether an Authorized User or the holder of an Independent Account, and never the Customer.

> The Ori Learning Definitions control the meaning of a capitalized term in every document listed above, except where a document at (a) or (b) defines the term for its own subject matter. An Order Form varies the Master Subscription Agreement only by language that identifies the section varied; a commercial field completed on the Order Form is not a variation. An Order Form varies the Data Privacy Addendum, a State Addendum, or an Exhibit only by language that identifies the section varied and is signed by both parties. A certification, disclosure or form that the Customer's law requires binds Ori Learning only where the Order Form identifies it or a signed amendment adopts it, and then as part of the Order Form. A purchase order's printed terms do not vary the Agreement. Nothing in this order of precedence limits a right or remedy that applicable law does not permit to be limited.

Nothing in the Agreement waives or limits Education Law §2-d or Part 121.

C.3 Compliance. Ori Learning is a third-party contractor under Education Law §2-d and complies with §2-d, 8 NYCRR Part 121 and the Customer's data security and privacy policy adopted under §121.5, as the Customer provides it to Ori Learning at contracting (Part B heading) and as later revised only where the revision is provided to Ori Learning and accepted as Master §15.3 provides, in its processing of the Customer's student data (§121.9(a)(1)–(2)).

C.4 Purposes and disclosure. Ori Learning uses personally identifiable information only for the exclusive purposes stated in Part A, element 1, which are the purposes the Agreement explicitly authorizes (§121.9(a)(4)), and limits internal access to those officers, employees and subcontractors who need it to provide the Services (§121.9(a)(3)). Ori Learning does not disclose personally identifiable information to any other party without the prior written consent of the parent or eligible student, except: to an authorized representative of Ori Learning, such as a subcontractor, to the extent it is carrying out the Agreement and in compliance with state and federal law, regulations and its contract with Ori Learning; to a recipient the Customer directs as part of Ori Learning's performance for the Customer, including the roster and sign-in providers the Customer elects under Data Privacy Addendum §9.1; to a successor that has assumed the Agreement and actually carries it out (Data Privacy Addendum §15.2); as required by statute; or by court order. Where a disclosure is required by statute or court order, Ori Learning gives the Customer notice no later than the disclosure unless notice is expressly prohibited (§121.9(a)(5)). The standing authorization in Data Privacy Addendum §14.2 to disclose personally identifiable information to emergency services or law enforcement does not apply to the Customer's data (§2-d(5)(f)(3); §121.9(a)(5)): where a person appears to be in imminent danger, Ori Learning refers the matter at once to the Customer's safety contact and its other designated contacts, and any disclosure under 34 C.F.R. §99.36 is the Customer's own to make and record. Ori Learning does not sell personally identifiable information and does not use, disclose, facilitate or permit its use for any marketing or commercial purpose (§121.9(a)(8)).

C.5 Security. Ori Learning maintains reasonable administrative, technical and physical safeguards to protect personally identifiable information (§121.9(a)(6)), aligns its technologies, safeguards and practices with the NIST Cybersecurity Framework 2.0 as Part B describes (§121.9(a)(1)), the framework being a reference and not a mapping or a conformance claim, encrypts personally identifiable information in motion and at rest as Part A, element 6, describes (§121.9(a)(7)), and requires each of its officers and employees, and those of its assignees, with access to complete training on the federal and state laws

governing confidentiality before access, as Part B describes (§121.6(a)(4)). The safeguards Part B describes are in place when the Customer's student data is received; where the Security & Incident Exhibit states a milestone for a safeguard it marks Adopted, that milestone applies to that safeguard alone.

C.6 Subcontractors. Ori Learning identifies its subcontractors on the Subprocessor Schedule, evaluates each before it receives the Customer's student data, binds it by written terms as Part B, B.5, describes, and remains responsible for it. Where Ori Learning engages a subcontractor to perform its obligations under the Agreement, the data protection obligations that state and federal law and the Agreement impose on Ori Learning apply to the subcontractor (§121.9(b)).

C.7 Breach and unauthorized release. Ori Learning notifies the Customer of any breach or unauthorized release of the Customer's personally identifiable information as Part B, B.6, states: in the most expedient way possible and without unreasonable delay, and no later than seven calendar days after discovery (§121.10(a)), with the content §121.10(g) lists; the notice under Section 11 of the Data Privacy Addendum carries the content that Section states, and the seven-day notice runs from discovery whether or not that notice has yet been given. Ori Learning cooperates with the Customer and with law enforcement (§121.10(c)). Where the breach or unauthorized release is attributed to Ori Learning or to a Subprocessor for which it is responsible, Ori Learning pays for or promptly reimburses the Customer for the full cost of the notifications §121.10 requires the Customer to give to parents, eligible students, teachers and principals (§121.10(f)). That obligation is a statutory obligation of Ori Learning, is not limited by Section 12.3 of the Master Subscription Agreement and is not excluded by Section 12.1 of it, and is the reimbursement for a New York Customer in place of the reimbursement in Section 11.8 of the Data Privacy Addendum; every other claim remains subject to Section 12 of the Master Subscription Agreement.

C.8 Students aged 13 to 17. For student data within Education Law §2-d, Ori Learning processes the Customer's student data only for the educational purposes the Agreement authorizes, on the §2-d basis, and no separate informed consent under the New York Child Data Protection Act (General Business Law article 39-FF) is sought for that processing. For any other personal data of a covered user aged 13 to 17 that Ori Learning processes, the basis is that the processing is strictly necessary for the purpose the Agreement authorizes or, failing that, informed consent (General Business Law §899-ff). General Business Law §899-gg applies to Ori Learning's processors in either case.

C.9 Requests, complaints and inspection. Requests by parents and eligible students to inspect and review student data are made to the Customer, which responds within 45 calendar days (§121.12); Ori Learning makes the records it holds available to the Customer within the period in Section 7.4 of the Data Privacy Addendum. Ori Learning cooperates with the Customer's complaint procedure under §121.4 and with any investigation, inspection or request of the Chief Privacy Officer under §121.11.

C.10 Publication. The Customer publishes Part A on its website as §121.3(d) requires. Ori Learning identifies the security-sensitive material it asks to have redacted; the determination of what redaction is necessary under §121.3(e) is the Customer's.

C.11 Term and execution. This Addendum takes effect when the Customer accepts the Order Form that incorporates it, or signs it where the Customer requires a signature, and continues for as long as the Data Privacy Addendum continues under its Section 15.1.

For the Customer (educational agency)	For Ori Learning
Name: Name	Name: Jonathan Izak
Title: Title	Title: Chief Executive Officer
Date: Date	Date: Date
Signature: Signature	Signature: Signature