VENDOR-SPECIFIC ('MODIFIED') STUDENT DATA PRIVACY AGREEMENT

(Oregon National Data Privacy Agreement (NDPA) Standard VERSION 2)

BEAVERTON SCHOOL DISTRICT

And

STONEWARE, INC

Version 2

Authored by Members of the Student Data Privacy Consortium (SDPC) &

Mark Williams, Fagen, Friedman & Fulfrost LLP

This Student Data Privacy Agreement ("DPA") is entered into on the date of full execution (the "Effective Date") and is entered into by and between:

[BEAVERTON SCHOOL DISTRICT],

located at [1260 NW WATERHOUSE AVE, BEAVERTON, OR 97006] (the "LEA")

and

[STONEWARE, INC],

located at [Stoneware, Inc., c/o Lenovo (United States) Inc., 8001 Development Drive, Morrisville, NC 27560] (the "Provider").

PREAMBLE

WHEREAS, the Provider is providing educational or digital Services, as defined in Exhibit "A", to LEA, which Services may include: (a) cloud-based Services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

WHEREAS, the Provider and LEA have entered into a Service Agreement (as defined herein), to provide certain Services to the LEA as set forth in the Service Agreement, and this DPA (collectively the "Agreement"),

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h; and the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6506 (16 C.F.R. Part 312),

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

LEA and Provider agree to the additional terms or modifications detailed in Exhibit "H".

Special Provisions. (Check if Required)

☐ If checked, the Supplemental State Terms attached hereto as Exhibit "G" are hereby incorporated by reference into this DPA in their entirety.

General Offer of Privacy Terms.

☑ If checked, the Provider has signed Exhibit "E" to the SDPC Standard Clauses, otherwise known as "General Offer of Privacy Terms" enabling other LEAs to enter into the same terms of this DPA with Provider.

The **designated representative for the LEA** for this DPA is:

Name: JAMES ALAN NEWTON Title: MANAGER OF APPLICATION DEVELOPMENT

Address: 1260 NW WATERHOUSE AVE, BEAVERTON, OR 97006

Phone: 503-356-4416 Email: JIM_NEWTON@BEAVERTON.K12.OR.US

The **designated representative for the Provider** for this DPA is:

Name: Dan Verwolf Title: Director, Product Management

Address: 8001 Development Drive, Morrisville, NC 27560

Phone: +1 (616) 284-1326 Email: dverwolf@lenovo.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: [BEAVERTON SCHOOL DISTRICT]

Signed By: James Alan Newton Date: Feb 27, 2025

Printed Name: JAMES ALAN NEWTON Title/Position: MANAGER OF APPLICATION DEVELOPMENT

PROVIDER: [STONEWARE, INC]

Signed By: Signed by: Dan Verwolf 765998272B724B1... Date: 27 February 2025

Printed Name: Dan Verwolf Title/Position: Director, Product Management

Each Party is responsible to promptly notify the other Party of changes to the notice information.

Notices to Provider

Name	STONEWARE, INC
Role	Privacy
Address	Stoneware, Inc., c/o Lenovo (United States) Inc., 8001 De
Email	privacy@lanschool.com

Notices to LEA

	BEAVERTON SCHOOL DISTRICT
	LEA Role
	1260 NW WATERHOUSE AVE, BEAVERTON, OR 97006
	IT-LEA-PRIVACY@BEAVERTON.K12.OR.US

With a copy to (if provided):

Name	
Address	
Email	

With a copy to (if provided):

	BEAVERTON SCHOOL DISTRICT
	1260 NW WATERHOUSE AVE, BEAVERTON, OR 97006
	IT-LEA-LEGAL@BEAVERTON.K12.OR.US

Security Notices to Provider (Required per Section 5.3)

Name	STONEWARE, INC
Role	Privacy
Address	Stoneware, Inc., c/o Lenovo (United States) Inc., 8001 De
Email	privacy@lanschool.com

Security Notices to LEA (Required per Section 5.3)

	BEAVERTON SCHOOL DISTRICT
	LEA Security Role
	1260 NW WATERHOUSE AVE, BEAVERTON, OR 97006
	IT-LEA-SECURITY@BEAVERTON.K12.OR.US

STANDARD CLAUSES

ARTICLE I: PURPOSE AND SCOPE

1.1 Purpose of DPA.

The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing Services otherwise provided by the LEA. With respect to its use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA as set forth in this DPA and the Service Agreement.

1.2 Description of Products and Services.

A description of all products and services covered by the Agreement, and information specific to this DPA, are listed in Exhibit "A". If a Provider needs to update any information on Exhibit “A” (such as updating with new provided services), they may do so by completing the Addendum template provided by the A4L Community and sending a copy to the LEA.

Provider may add or delete products or services subject to this DPA under the following circumstances:

1. Deleted products or services: The products or services have been discontinued and are no longer available from the Provider.
2. Added products or services: The added products or services are either:
    a. a direct replacement, or substantially equivalent to the original products or services listed in the DPA, or
    b. the added products or services result in enriched new or enhanced capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed.

If an added product or service requires additional Data Elements, Provider must complete the relevant portion of the Addendum template to update Exhibit “B”.

Provider may not make any change to Exhibit “A” via an Addendum, except adding or deleting products or services. LEA is under no obligation to acquire added products or services, and has no ability under the DPA to prevent deletion of products or services. Subject to the limitations in this section, an Addendum is automatically incorporated into this DPA when LEA is notified by Provider, in accordance with the notification provisions of this DPA, of the Addendum’s existence and contents.

1.3 Student Data to Be Provided.

In order to perform the services, the Provider shall process Student Data as identified by the Provider in the Schedule of Data, attached hereto as Exhibit “B”. Student Data may be provided by the LEA or created by students, as set forth fully in the definition of Student Data in Exhibit “C”. If a Provider needs to update any information on Exhibit “B”, they may do so by completing the Addendum template provided by the A4L Community and sending a copy to the LEA.

Provider may delete data elements from Exhibit “B” if they are no longer used by the Provider.

Provider must add data elements to Exhibit "B", when a material change has occurred, regardless of whether the added data elements are either one of the following:

1. used to better deliver the original products or services listed in the DPA, or
2. used to deliver added products or services that result in new or enhanced capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed. Such new products or services must be designated in the Addendum template as changes to Exhibit "A".

The Provider must notify the LEA, in accordance with the notification provisions of this DPA, of the existence and contents of an Addendum modifying Exhibit "B". The LEA will have thirty (30) days from receipt to object to the Addendum. If no written objection is received it will become incorporated into the DPA between the parties.

1.4 DPA Definitions.

Capitalized terms used in this DPA shall have the meanings set forth in Exhibit "C". With respect to the treatment of Student Data, in the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to, the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1 Student Data Property of LEA.

As between LEA and Provider, all Student Data processed by the Provider, or created by students (as set forth fully in the definition of Student Data in Exhibit "C"), pursuant to the Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data processed by the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA.

2.2 Parent, Legal Guardian and Student Access.

The LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student (as defined in FERPA) may review Student Data and request deletion or modification, and request delivery of a copy of the Student Data. In support of this, the Provider shall establish reasonable procedures by which the LEA may access, and correct if necessary, Education Records and/or Student Data, and make a copy of the data available to the LEA or (at the LEA's direction) to the parent, legal guardian or eligible student directly. If the LEA is not able to review or update the Student Data itself, Provider shall respond in a reasonably timely manner (and no later than thirty (30) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent, legal guardian or student, whichever is sooner) to the LEA's request for Student Data held by the Provider to view or correct as necessary.

In the event that a parent or legal guardian of a student or eligible student contacts the Provider to correct, delete, review or request delivery of a copy of any of the Student Data collected by or generated through the Services, the Provider shall refer that person to the LEA, who will follow the necessary and proper procedures regarding

the requested information. In the event that any person other than those listed contacts the Provider about any Student Data, the Provider shall refer that person to the LEA, except as provided in Section 4.4.

2.2.1 This NDPA does not impede the ability of students to download, export, or otherwise save or maintain their own Student Generated Content directly from Provider or for Provider to provide a mechanism for such download, export, transfer or saving to students, or the student's parent or legal guardian. Nor does it impede the ability of Providers to offer LEAs features to allow such ability.

2.2.2 In the event that Student Generated Content is transferred to the control of the student, parent or legal guardian, the copy of such Student Generated Content that is in the control of such person is no longer considered Student Data.

2.3 Subprocessors.

Provider shall enter into a Subprocessor Agreement with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA. Every Subprocessor Agreement must provide that the Subprocessor will not Sell the Student Data. The terms of a Subprocessor Agreement shall not be materially modified by the Subprocessor unless notice is provided to the Provider.

ARTICLE III: DUTIES OF LEA

3.1 Provide Data in Compliance with Applicable Laws.

LEA shall use the Services and provide Student Data in compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time.

3.2 Annual Notification of Rights.

If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.

3.3 Reasonable Precautions.

LEA shall employ administrative, physical, and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted Student Data from unauthorized access, disclosure, or acquisition by an unauthorized person.

3.4 Unauthorized Access Notification and Assistance.

LEA shall notify Provider within seventy-two (72) hours of any confirmed Data Breach to the Services, LEA's account or any Student Data that poses a privacy or security risk. If requested by Provider, LEA will provide reasonable assistance to Provider in any efforts by Provider to investigate and respond to such Data Breach.

ARTICLE IV: DUTIES OF PROVIDER

4.1 Privacy and Security Compliance.

The Provider shall comply with all laws and regulations applicable to Provider's protection of Student Data privacy and security, and at the direction of the LEA shall cooperate with any state or federal government initiated audit of the LEA's use of the Services.

4.2 Authorized Use.

The Student Data processed pursuant to the Services shall be used by the Provider for no purpose other than performing the Services outlined in Exhibit "A", or as instructed by the LEA.

4.3 Provider Employee Obligation.

Provider shall require all of Provider's employees who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee with access to Student Data pursuant to the Service Agreement.

4.4 No Disclosure.

Provider acknowledges and agrees that it shall not sell or disclose any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data.

4.4.1 Exceptions to No Disclosure.

4.4.1.1 This prohibition against disclosure will not apply to Student Data where disclosure is directed or permitted by the LEA or this DPA.

4.4.1.2 The provision to not sell Student Data shall not apply to a Change of Control.

4.4.1.3 This prohibition against disclosure shall not apply to Student Data disclosed pursuant to a judicial order or lawfully issued subpoena or warrant.

4.4.1.4 This prohibition against disclosure shall not apply to Student Data disclosed to Subprocessors performing Services on behalf of the Provider pursuant to this DPA.

4.4.1.5 Should law enforcement or other government entities ("Requesting Party(ies)") provide a judicial order or lawfully issued subpoena or warrant to the Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party.

4.4.1.6 Notification under 4.4.1.5 is not required if the judicial order or lawfully issued subpoena or warrant states not to inform the LEA of the request.

4.4.1.7 Should the LEA be presented with a judicial order or lawfully issued subpoena or warrant to disclose Student Generated Content or other Student Data, the Provider shall cooperate with the LEA in delivering such data.

4.4.1.8 This prohibition against disclosure shall not apply to LEA-authorized users of the Services, which may include parents and legal guardians.

4.4.1.9 This prohibition against disclosure shall not apply to protect the safety of users or others, if and only if, an LEA employee who has specifically been authorized to declare a health or safety emergency has done so and all requirements under 34 CFR §§ 99.31(a)(10) and 99.36 have been fulfilled by the LEA.

4.4.1.10 This prohibition against disclosure shall not apply to protect the integrity or security of the Service, where such disclosure is made to a Subprocessor engaged by Provider for the specific purpose of investigating a potential Data Breach as set forth in 5.4.

4.5 De-Identified Data

Provider agrees not to attempt to re-identify De-Identified Student Data without the written direction of the LEA. De-Identified Student Data may be used by the Provider for those purposes allowed under applicable laws, for the purposes allowed for the processing of Student Data under this DPA, as well as the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; (2) research, development, and improvement of the Provider's educational sites, Services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Student Data shall survive termination of this DPA or any request by LEA to return or dispose of Student Data. Except for Subprocessors, Provider agrees not to transfer De-identified Student Data to any third party unless the transfer is expressly directed or permitted by the LEA or this DPA. Such Subprocessors must be subject to equivalent terms of the DPA including this one. Prior to publishing any document that names the LEA, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Student Data is presented. If Provider chooses to create De-Identified Data, its process must comply with either NIST de-identification standards or US Department of Education guidance on de-identification.

4.6 Disposition of Data.

Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree.

If the Provider has a standard retention and destruction schedule, that schedule shall apply to Student Data as long as this DPA is active. The Provider's practice relating to retention and disposition of Student Data shall be provided to the LEA upon request.

At the termination of this DPA, the Provider shall, unless directed otherwise by the LEA, dispose of, or delete Student Data obtained by the Provider under the Agreement within sixty (60) days of termination (unless otherwise required by law). If the Agreement has lapsed or is not terminated, the Student Data shall be deleted when directed or permitted by the LEA, according to Provider's standard destruction schedule, or as otherwise required by law. The LEA may provide the Provider with special instructions for the disposition of the Student Data, by transmitting to Provider Exhibit "D", attached hereto. The duty of the Provider to dispose of or delete Student Data shall not extend to De-Identified Data or to Student-Generated Content that has been transferred or kept pursuant to Section 2.2.2.

4.7 Advertising Limits.

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA; or (c) for any commercial purpose other than to provide the Service to the LEA, or as authorized by the LEA or the parent/guardian. Targeted Advertising is strictly prohibited. However, this section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to account holders that are not considered Targeted Advertising (this exception does not apply where the Provider is relying on the LEA to provide consent on behalf of the parent under COPPA); or (iii) to notify account holders about new education product updates, features, or Services that are not considered Targeted Advertising or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

Before making product recommendations under section (ii) above, Provider must disclose the existence of those recommendations to LEA in writing, in sufficient detail that LEA can fulfill any obligations under applicable law (e.g. PPRA).

ARTICLE V: DATA SECURITY AND BREACH PROVISIONS

5.1 Data Storage.

If Student Data is stored outside the United States, Provider will provide a list of Countries where data is stored, in Exhibit “B”.

5.2 Security Audits.

Provider will conduct a security audit or assessment no less than once per year, and upon a Data Breach. Upon 10 days’ notice and execution of confidentiality agreement, Provider will provide the LEA with a copy of the audit report, subject to reasonable and appropriate redaction.

5.3 Data Security.

The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security of Student Data. The Provider shall implement an adequate Cybersecurity Framework that incorporates one or more of the nationally or internationally recognized standards set forth in Exhibit “F”. Additionally, Provider may choose to further detail its security programs and measures in Exhibit “F”. Provider shall provide, in the Preamble to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

5.4 Data Breach.

In the event that Provider confirms a Data Breach, the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the Data Breach, unless notification within these time limits would disrupt investigation of the Data Breach by law enforcement. In such an event, notification shall be made within a reasonable time after the Data Breach. Provider shall follow the following process:

(1) The Data Breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

- (a) The name and contact information of the Provider subject to this section,
- (b) the date of the notice,
- (c) the date of the Data Breach, the estimated date of the Data Breach, or the date range within which the Data Breach occurred,
- (d) Whether the notification was delayed as a result of a law enforcement investigation, if legally permissible to share that information,
- (e) A general description of the Data Breach, if that information is possible to determine at the time the notice is provided,
- (f) A description of the Student Data reasonably believed to have been the subject of the Data Breach; and
- (g) Identification of impacted individuals.

(2) Provider agrees to adhere to all applicable federal and state laws with respect to a Data Breach related to the Student Data, including any required responsibilities and procedures for notification and mitigation of any such Data Breach.

(3) Provider further acknowledges and agrees to have a written Data Breach response plan that is consistent with applicable industry standards and federal and state law for responding to a Data Breach, involving Student Data and agrees to provide LEA, upon reasonable written request, with a summary of said written Data Breach response plan.

(4) LEA shall provide notice and facts surrounding the Data Breach to the affected students, parents, or guardians.

(5) In the event of a Data Breach originating from LEA's use of the Service or otherwise a result of LEA's actions or inactions, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data and may request costs incurred as a result of such Data Breach.

CONTRACT TERMS

Term and Termination. In the event that either Party seeks to terminate this DPA, they may do so by written notice if the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any Service Agreement or contract if the other party breaches any terms of this DPA. This DPA shall stay in effect for as long as the Provider retains the Student Data, as set forth in section Article IV, Section 4.6. In the case of a "Change of Control" the LEA has the authority to terminate the DPA if it reasonably believes that the successor cannot uphold the terms and conditions herein or having a contract with the successor would violate the LEA's policies or state or federal law.

Data Disposition on Service Agreement Termination. If the Service Agreement is terminated, the Provider shall dispose of all of LEA's Student Data pursuant to Article IV, Section 4.6 of the Standard Clauses.

Notices. All notices or other communication required or permitted to be given hereunder must be made in writing and may be given via e-mail transmission, or first-class mail, or mutually agreed upon method sent to the designated representatives documented in the Preamble.

Priority of Agreements. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. With respect to the treatment of Student Data only, in the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit "H", the SDPC Standard Clauses, and/or the Supplemental State Terms in Exhibit "G", Exhibit "H" will control, followed by Exhibit "G". Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

Entire Agreement. This DPA and the Service Agreement ("the Agreement") constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties.

Severability. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

Governing Law; Venue and Jurisdiction. This DPA will be governed by and construed in accordance with the laws of the state of the LEA, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction to the state and federal courts for the county of the LEA for any dispute arising out of or relating to this DPA or the transactions contemplated hereby.

Successors Bound. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a Change of Control. In the event of a Change of Control, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of such Change of Control. Such notice shall include

a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement.

Authority. Each signatory confirms they are authorized to bind their institution to this DPA in its entirety.

Waiver. No delay or omission by either party to exercise any right here under shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT A: PRODUCTS AND SERVICES

This DPA covers access to and use of [STONEWARE, INC]'s existing Services that collect, process, or transmit Student Data, as identified below:

LanSchool Air and LanSchool Classic

EXHIBIT B: SCHEDULE OF STUDENT DATA

All Data Elements identified in this Exhibit are correct at time of signature.

Data Elements Collected by Product (required and optional):

Category of Data / Data Elements	**LanSchool Air**	**LanSchool Classic**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**
Application Technology MetaData							
IP Addresses of users, use of cookies, etc.	X						
Other application technology metadata	X						
If 'Other' checked, please specify below checked box:							
Application Use Statistics							
Meta data on user interaction with application	Please refer to our LanSchool Air DPA: https://files.lenovosoftware.com/privacy/LanSchool-Air-Data-Processor-Agreement.pdf						
Assessment							
Standardized test scores							
Observation data							
Voice recordings							
Other assessment data							
If 'Other' checked, please specify below checked box:							
Attendance							
Student school (daily) attendance data							

Category of Data / Data Elements	**LanSchool Air**	**LanSchool Classic**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**
Student class attendance data							
Communication							
Online communication captured (emails, blog entries)	X						
Conduct							
Conduct or behavioral data							
Demographics							
Date of birth							
Place of birth							
Gender							
Ethnicity or race							
Language information (native, or primary language spoken by student)							
Other demographic information							
If 'Other' checked, please specify below checked box:							
Enrollment							
Student school enrollment	X						
Student grade level	X						
Homeroom							
Guidance counselor							
Specific curriculum programs							
Year of graduation							

Category of Data / Data Elements	**LanSchool Air**	**LanSchool Classic**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**
Other enrollment information							
If 'Other' checked, please specify below checked box:							
Parent/Guardian Contact Information							
Address							
Email							
Phone							
Parent/Guardian ID							
Parent ID number (created to link parents to students)							
Parent/Guardian Name							
First and/or last							
Schedule							
Student scheduled courses	x						
Teacher names	x						
Special Indicator							
English language learner information							
Low-income status							
Medical alerts/health data							
Student disability information							
Specialized education Services (IEP or 504)							
Living situations (homeless/foster care)							
Other indicator information							

Category of Data / Data Elements	**LanSchool Air**	**LanSchool Classic**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**	**PRODUCT NAME(S)**
If 'Other' checked, please specify below checked box:							
Student Contact Information							
Address							
Email	x						
Phone							
Student Identifiers							
Local (school district) ID number	x						
State ID number							
Provider/app assigned student ID number	x						
Student app username	x						
Student app passwords	x						
Student Name							
First and/or last							
Student In App Performance							
Program/application performance (e.g. typing program – student types 60 wpm, reading program – student reads below grade level)							
Student Program Membership							
Academic or extracurricular activities a student may belong to or participate in							

Student Survey Responses							
Student responses to surveys or questionnaires							
Student Work							
Student generated content; writing, pictures, etc.							
Other student work data							
If 'Other' checked, please specify below checked box:							
Transcript							
Student course grades							
Student course data							
Student course grades/performance scores							
Other transcript data							
If 'Other' checked, please specify below checked box:							
Transportation							
Student bus assignment							
Student pick up and/or drop off location							
Student bus card ID number							
Other transportation data							

If 'Other' checked, please specify below checked box:							
Other							
Other data collected	x						
If 'Other' checked, please list each additional data element used, stored, or collected by your application below checked box:	Please refer to our LanSchool Air DPA: https://files.lenovosoftware.com/privacy/LanSchool-Air-Data-Processor-Agreement.pdf						
None							
No student data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.							

If Student Data is stored outside the United States, Provider shall list below the Countries where data is stored:

EXHIBIT C: DEFINITIONS

Change of Control: Any merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of Provider or of the portion of Provider that performs the Services in the Service Agreement.

Contextual Advertising: Contextual advertising is the delivery of advertisements based upon a current visit to a Web page or a single search query, without the collection and retention of data about the consumer's online activities over time.

De-Identified Data: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific student, including, but not limited to, any information that, alone or in combination is linkable to a specific student.

Data Breach: An unauthorized release, access to, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider in violation of applicable state or federal law.

Educational Records: Educational Records shall have the meaning set forth under FERPA 20 U.S. C. 12 32 g(a)(5)(A). For additional context see also the 'Student Data' definition.

LEA: For the purpose of this DPA, the LEA is the educational entity that is a Party to this Agreement. An LEA can be a state agency, an educational service agency, a charter school or school system or a private school or school system, in addition to the federal definition of Local Education Agency (LEA).

Metadata: Means information that provides meaning and context to other data being collected including, but not limited to date and time records and purpose of creation. Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information or Student Data.

Originating LEA: An educational entity otherwise meeting the definition of LEA that originally executes the DPA in its entirety (including the marked checkbox enabling Exhibit "E") with the Provider.

School Official: For the purposes of this DPA and pursuant to FERPA 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Educational Records; and (3) Is subject to FERPA 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Educational Records.

Service Agreement: Refers to the quote, corresponding contract, purchase order or terms of service and/or terms of use.

Student Data: Student Data includes any data, whether gathered, created or inferred by Provider or provided by LEA or its users, students, or students' parents/guardians, for a school purpose, that is descriptive of the student including, but not limited to, information in the student's Educational Record, persistent unique identifiers, or any other information or identification number that would provide information about a specific student. Student Data includes Metadata that has not been stripped of all direct and indirect identifiers. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed

to be collected or processed by the Provider pursuant to the Services. Student Data shall not include properly De- Identified Data or anonymous usage data regarding a student's or LEA's use of Provider's Services.

Student Generated Content: The term "Student Generated Content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content. "Student Generated Content" does not include student responses to a standardized assessment where student possession and control would jeopardize the validity and reliability of that assessment.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to or storage of Student Data, including security, storage, analytics, and other processing activities necessary to perform a Provider business purpose.

Subprocessor Agreement: An agreement between Provider and a third party Subprocessor. A Subprocessor Agreement includes either a written agreement or an acceptance of terms and conditions (e.g., click through agreements).

Subscribing LEA: An educational entity otherwise meeting the definition of LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms by executing Exhibit "E".

Targeted Advertising: Targeted Advertising means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the Provider Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include Contextual Advertising.

EXHIBIT D: SPECIAL INSTRUCTIONS FOR DISPOSITION OF DATA

After this DPA takes effect, if the LEA has special requirements for the disposition of Student Data that are not expressed in 4.6 Disposition of Data, the LEA may fill in this form and deliver it to the Provider.

The Provider and the LEA must not fill in this form at the initiation of the DPA.

The Provider shall act on Exhibit "D" from the designated representative of the LEA or their designee (Preamble or Exhibit "E" for Subscribing LEA).

BEAVERTON SCHOOL DISTRICT ("LEA") instructs Provider to dispose of Student Data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. **Extent of Disposition**
   - ☐ Disposition is partial. The scope of Student Data to be disposed of is set forth below or found in an attachment to this Directive:
     Insert categories of Student Data here
   - ☐ Disposition is complete. Disposition extends to all Student Data.
2. **Nature of Disposition**
   - ☐ Disposition shall be by destruction or deletion of Student Data.
   - ☐ Disposition shall be by a transfer of Student Data. The Student Data shall be transferred to the following site as follows:
     Insert of attach special instructions
3. **Timing of Disposition**
   Student Data shall be disposed of by the following date:
   - ☐ As soon as commercially practicable
   - ☐ On Provider's standard destruction schedule
   - ☐ By Insert Date
4. **De-Identified Data**
   - ☐ The Provider certifies that they have De-Identified the data, as defined elsewhere in this Agreement, and disposed of all copies of Student Data that were not De-Identified in accordance with this Schedule and the DPA. The Provider will notify LEA in accordance with the notification requirements of the DPA using this form.
     As of Enter Date
5. **Other:**

Signature(s)		**Notice of Verified Disposition of Data**	
Authorized Representative of LEA	Date	Authorized Representative of Provider	Date

EXHIBIT E: GENERAL OFFERS OF TERMS

Page 1 of 2: OFFER OF TERMS

Provider and the Subscribing LEA (named below) agree by signing this General Offer of Privacy Terms ("General Offer") that they are bound by the same terms as the DPA between Provider and BEAVERTON SCHOOL DISTRICT ("**Originating LEA**") dated _____.

Provider and Subscribing LEA agree that the information below will be replaced throughout the DPA with the information specific to the Subscribing LEA filled in below for the Subscribing LEA. This General Offer shall extend only to the terms set forth in this DPA and shall not necessarily bind Provider or Subscribing LEA to any other terms entered into between Provider and Originating LEA. Any commercial terms, such as price, term, or schedule of Services, relating to Subscribing LEA's use of the Provider's Services shall be determined solely between Provider and Subscribing LEA.

If Provider makes changes to Exhibit "A" or Exhibit "B" in accordance with sections 1.2 and 1.3 respectively, Provider must complete the Addendum template provided by the A4L Community and notify the Originating LEA and all Subscribing LEAs in accordance with the notification provisions of this DPA, of the Addendum's existence and contents. With regard to a Subscribing LEA, an Addendum is automatically incorporated into this DPA when Subscribing LEA is notified by Provider. If an Addendum modifies Exhibit "B", the LEA will have thirty (30) days from receipt to object. If no written objection is received it will become incorporated into the DPA between the parties.

The Provider may withdraw the General Offer (for future use or for LEAs that have not already accepted it) in the event of: (1) a material change in the applicable privacy statutes; or (2) a material change in the Services and products listed in the Service Agreement. Notification of a withdrawal shall be submitted to ndpa_requests@A4L.org.

Subscribing LEAs shall send the signed Exhibit "E" to Provider at the following email address: privacy@lanschool.com

The below signatory confirms they are authorized to bind their institution to this DPA as in its entirety.

RESOURCE NAME(S):

[LanSchool Air and LanSchool Classic]
[ ]
[ ]
[ ]

PROVIDER: [STONEWARE, INC]

Signed By: Signed by: Dan Verwolf 765008272B724B1... Date: 27 February 2025

Printed Name: Dan Verwolf Title/Position: Director, Product Management

Exhibit "E" (continued)

Originating LEA: BEAVERTON SCHOOL DISTRICT
Resource Names: LanSchool Air and LanSchool Classic
Provider Name: STONEWARE, INC

Page 2 of 2:

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Originating LEA and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER.**** Please note, by signing this Exhibit you are also agreeing to any language that may be included in Exhibits to the Originating DPA beyond this Exhibit "E". The below signatory confirms they are authorized to bind their institution to this DPA as in its entirety.

Subscribing LEA: Insert Name of Subscribing LEA

Signed By: _____ Date: _____

Printed Name: _____ Title/Position: _____

School District Name: _____

Designated Representative of LEA:

Name: JAMES ALAN NEWTON Title: MANAGER OF APPLICATION DEVELOPME

Address: 1260 NW WATERHOUSE AVE, BEAVERTON, OR 97006

Telephone: 503-356-4416 Email: JIM_NEWTON@BEAVERTON.K12.OR.US

Notices to Subscribing LEA: The Provider and Subscribing LEA are each responsible to promptly notify the other Party of changes to the notice information.

Security Notices to Subscribing LEA

Name Stoneware, Inc.
Role LEA Security Role
Address 8001 Development Drive, Morrisville, NC 27560
Email privacy@lanschool.com

Name Stoneware, Inc.
Role LEA Role
Address 8001 Development Drive, Morrisville, NC 27560
Email privacy@lanschool.com

With a copy to (if provided):
Name
Address LEA Legal Counsel Postal Address
EMail

EXHIBIT F: ADEQUATE CYBERSECURITY FRAMEWORKS

Provider must mark one or more frameworks with which it complies.

The Provider may change which framework it complies with without invalidating or changing the DPA, but must notify the LEA of such change in accordance with the notification requirements of the DPA.

FRAMEWORK(S)	
☐	Global Education Security Standard - https://sdpc.a4l.org/gess/
☐	NIST Cybersecurity Framework (CSF)
☐	NIST SP 800-53 Security and Privacy Controls for Information systems and organizations
☐	NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
☐	ISO 27000 series, Standards for implementing organization security and management practices
☐	CIS Center for Internet Security Critical Security Controls
☐	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

This space is provided for optional security programs and measures as noted in section 5.3:

See attached Stoneware security program and administrative controls.

Stoneware has implemented a comprehensive and written security program with physical, technical, procedural, and administrative controls that reflect prevailing industry standards for the protection and responsible use of Personal Data including, but not limited to, the following controls:

Technical	Scope	Controls
Access	Logins (system & application).	NIST-based password policies (multi-factor authentication for admin-level access and interfaces).
Encryption	Data storage at rest & in transit.	AES 256-GCM (at rest), TLS 1.2 (in transit) Protocol TLS 1.3 (in transit) Supported TLS Ciphers TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 (server preferred cipher suites).
Static application security testing	All server and micro-service images, All binary clients and extensions/plugins.	Regular vulnerability scans and monitoring.
Dynamic application security testing	External applications APIs.	Web application scans, Penetration testing (Regular internal tests.)
CIS benchmark hardening	Cloud platform provider, Server instances.	Cloud CIS compliance checks, Cloud security monitoring, Regular CIS L2 server benchmark assessments.
Software compositional analysis	3rd party opensource dependencies.	Conduct regular vulnerability audits, repository monitoring.
Infrastructure assessment	Cloud platform provider.	Regular reviews of all software-defined networks (SDNs) (identify network segmentation, firewall configuration, and resource access misconfigurations).
Web application firewall (WAF)	Production web applications.	WAF protection (core rules for common attacks).
Static code analysis	Proprietary code.	Regular code analysis is conducted using a commercial tool, secure code reviews are conducted during code merges.
Log collection	Cloud platform provider, Application.	Cloud platform API transactions (logs older than 360-days are purged, accessible by engineering), WAF logging for edge detection (logs older than 90-days are purged, accessible by engineering), Subprocessors, see Annex B, for application purposes.
Infrastructure as code	Cloud platform provider.	Infrastructure as code is used to automate infrastructure deployments and improve the immutability, misconfiguration of infrastructure.
Incident (including data breach) response	Security events related to products in production.	Product incident response plan in accordance with NIST 800-61 and Lenovo's internal Product Security Incident Response Team (PSIRT) processes.

Organizational	Scope	Controls
Trusted providers list	All subprocessors that directly integrate with products in production.	Standard security assessments of integrated providers, DPAs for Personal Data processing providers.
Vulnerability management	Server OSes, Docker containers, Clients, Products in production.	A program that employs various tools to aid in identifying vulnerabilities across all compute systems.
Software Security Review Board (SSRB)	Products in production.	SSRB reviews are conducted regularly. During reviews, all technical and organizational measures are assessed for the product in question.
Data retention policy	Personal identifiable information, Application data, Products in production.	Upon user's request for deletion or after one year of not having an active license or trial, personal data will be archived. Archived data is purged after 90 days.
Security and privacy awareness	All employees (Privacy Basics and Security Essentials courses)	Semi-annual training for specialized IT and product teams on advanced security topics, such as OWASP Top 10.
Continuous security	Products in production.	Regular application of Technical Measures.
Opensource compliance reviews.	Products in production.	Assessments conducted to ensure proper licensing and attributions are provided in distributed software.
Disaster Recovery	Products in production	Following NIST-800-34 as a guide to maximize RTO and RPO.
Backup policy	Databases, Code, Logs.	The general policy requires multiple backups, one of which must be offsite from the primary storage location, Regular database backups occurring daily (2 times per day), weekly, and monthly. Daily backups are retained for 7 days. Weekly backups are retained for 4 weeks. Monthly backups are retained for 13 months. The restore window is 12 hours. Application source code backups occur daily and are retained for 360 days. Production logs: Datadog – Logs are live for 7 days. Logs are then put in long-term storage for 180 days and then purged. Load Balancer – Logs are retained for 360 days and then purged. Web Application Firewall – Logs are retained for 90 days and then purged. Cloud Trail – Logs are retained for 90 days and then purged. Cloud Watch – Logs are retained for 360 days and then purged. MongoDB – Logs are retained for the life of the project.

EXHIBIT G: Supplemental SDPC State Terms for Oregon

[The State Supplement is an optional set of terms that will be generated on an as-needed basis to meet state specific data privacy statute requirements. The scope of these State Supplements will be to cite and address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (Exhibit "H" in this proposed structure).]

EXHIBIT H: DESCRIPTION OF 'AGREED TO' CHANGES

LEA and Provider agree to the following additional or replacement terms and modifications:

PREAMBLE WHEREAS, the Provider and LEA have entered into ~~a Service Agreement (as defined herein),~~ the LanSchool Air Terms of Service ("Service Agreement") to provide certain Services to the LEA as set forth in the Service Agreement, and this DPA (collectively the “Agreement”),

2.21 and 2.22 – strike entirely – Comments: We do not allow for Student-Generated Content to be saved, nor made available to students or teachers to see or access. Student generated content would be things they create and store in the app that they "own" and therefore would expect the ability to take with them outside of LanSchool. We don't have anything like that.

3.3 Reasonable Precautions. LEA shall employ reasonable administrative, physical, and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted Student Data from unauthorized access, disclosure, or acquisition by an unauthorized person.

4.1 Privacy and Security Compliance The Provider shall comply with all laws and regulations applicable to Provider’s protection of Student Data privacy and security, and at the direction of the LEA shall reasonably cooperate with any state or federal government initiated audit of the LEA’s use of the Services.

4.5 De-Identified Data ....Prior to publishing any document that names the LEA, the Provider shall obtain the LEA’s written approval of the manner in which De-Identified Student Data is presented. If Provider chooses to create De-Identified Data, its process ~~must~~ will comply with either ~~NIST~~ industry de-identification standards or US Department of Education guidance on de-identification.

4.6 Disposition of Data Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) business days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. . . .

At the termination of this DPA, the Provider shall, unless directed otherwise by the LEA, dispose of, or delete Student Data obtained by the Provider under the Agreement within sixty (60) business days of termination (unless otherwise required by law).

5.2 Security Audits. Provider will conduct a security audit or assessment no less than once per calendar year, and upon a Data Breach. Upon ~~10~~ 30 days’ written notice and execution of confidentiality agreement, Provider will provide the LEA with a copy of the audit report, subject to reasonable and appropriate redaction.

5.3 Data Security. The Provider agrees to utilize reasonable administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law(s) relating to data security of Student Data. . . . .

5.4 Data Breach.
In the event that Provider confirms a Data Breach, the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the Data Breach, unless notification within these time limits would disrupt investigation of the Data Breach by law enforcement. In such an event, notification shall be made within a commercially reasonable time after the Data Breach. Provider shall follow the following process: .. . . .
(5) In the event of a Data Breach originating from LEA’s use of the Service or otherwise a result of LEA’s actions or inactions, Provider shall reasonably cooperate with LEA to the extent necessary to ~~expeditiously~~ promptly secure Student Data. LEA ~~and~~ may request reasonable costs incurred as a result of such Data Breach, in instances where Provicdr is determined to have caused such Breach.

5.5 Limitation of Liability. Provider’s liability under this DPA will be subject to the liability terms and conditions under the Service Agreement.

Term and Termination. In the event that either Party seeks to terminate this DPA, they may do so by written notice if the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any Service Agreement or contract if the other party breaches any terms of this DPA, and has failed to cure the alleged breach within thirty (30) days afer receiving notice of the alleged breach. This DPA shall stay in effect for as long as the Provider retains the Student Data, as set forth in section Article IV, Section 4.6. In the case of a “Change of Control” the LEA has the authority to terminate the DPA if it reasonably believes that the successor cannot uphold the terms and conditions herein or having a contract with the successor would violate the LEA’s policies or state or federal law.

Lenovo DPA

Final Audit Report 2025-02-28

Created:	2025-02-27
By:	leslie erickson (leslie_erickson@beaverton.k12.or.us)
Status:	Signed
Transaction ID:	CBJCHBCAABAAWOqhlVYf8lb7pU2TY_s8CnOkK3idkhHB

"Lenovo DPA" History

Document digitally presigned by DocuSign\, Inc. (enterprisesupport@docusign.com)
2025-02-27 - 5:37:06 PM GMT- IP address: 66.154.176.206

Document created by leslie erickson (leslie_erickson@beaverton.k12.or.us)
2025-02-27 - 5:50:52 PM GMT- IP address: 66.154.176.206

Document emailed to jim newton (jim_newton@beaverton.k12.or.us) for signature
2025-02-27 - 5:52:23 PM GMT

Email viewed by jim newton (jim_newton@beaverton.k12.or.us)
2025-02-28 - 2:56:34 AM GMT- IP address: 67.1.197.57

Document e-signed by jim newton (jim_newton@beaverton.k12.or.us)
Signature Date: 2025-02-28 - 3:00:22 AM GMT - Time Source: server- IP address: 67.1.197.57

Agreement completed.
2025-02-28 - 3:00:22 AM GMT