

RULE 6A-1.0955 and 6A-1.09550 AMENDMENT

Student DPA - Florida Virtual School

THIS RULE 6A-1.0955 and 6A-1.09550 AMENDMENT is made by and between Florida Virtual School, a political subdivision of the State of Florida (“**Florida Virtual School**”) and Zoom Communications, Inc. (“**Provider**”), and is intended to modify the Terms of Service, Master Subscription Agreement, or any other agreement previously entered into by Florida Virtual School and Provider with respect to Provider’s delivery of the contracted services (the “**Prior Agreement**”). Florida Virtual School and Provider may also be referred to herein each as a “**Party**” and collectively as the “**Parties**”.

WHEREAS, Florida Virtual School is responsible for operating a Florida statewide, internet-based public K-12 school system.

WHEREAS, Rules 6A-1.0955 and 6A-1.09550 of the Florida Administrative Code were promulgated by the Florida Department of Education with effective dates of February 20, 2024 and September 26, 2023, respectively (the “**Rules**”).

WHEREAS, the Rules require certain additional terms and conditions be incorporated into all existing and future agreements that involve or may involve any disclosure or use of student personally identifiable information (“**PII**”).

WHEREAS, Florida Virtual School and Provider believe the Prior Agreement may be subject to the Rules.

NOW, THEREFORE, in consideration of the premises and of the mutual covenants contained herein and to bring the Prior Agreement into compliance with the Rules, the Parties hereby agree to amend and modify the Prior Agreement as follows:

1. The above Recitals are incorporated herein by reference.
2. Attachment “A” below, including all exhibits attached thereto, is fully incorporated into and made a part of the Prior Agreement.
3. Provider shall promptly notify Florida Virtual School in writing concerning needed updates to Attachment “A”, Exhibit “B” (Schedule of Data) due to any material changes that impact the disclosure or use of PII (“**Needed Changes**”), after which the Parties shall modify said Exhibit “B” accordingly. Failure by Provider to notify Florida Virtual School of any Needed Changes shall constitute default and a material breach of the Prior Agreement and provide Florida Virtual School the option, but not the obligation, to immediately terminate the Prior Agreement without penalty. For clarification, any optional features that Provider may offer for the SDPA Services which LEA may choose to add to the SDPA Services do not constitute Needed Changes.
4. The effective date of this Amendment shall be the date of full execution by the Parties.
5. This Amendment may be executed in counterparts, whether signed physically or electronically, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

ATTACHMENT A

STUDENT DATA PRIVACY AGREEMENT

THIS STUDENT DATA PRIVACY AGREEMENT (“**SDPA**”), as developed by the Student Data Privacy Consortium (“**SDPC**”) and modified by the local education agency identified herein, is entered into on the date of full execution (the “**Effective Date**”) by and between The Florida Virtual School, a political subdivision of the State of Florida and designated local education agency for purposes of this SDPA (“**LEA**”) and Zoom Communications, Inc. (“**Provider**”). LEA and Provider may also be referred to herein each as a “**Party**” and collectively as the “**Parties**”.

WHEREAS, Provider is obligated under that certain Master Subscription Agreement or terms of service by and between Provider and LEA (the “**Service Agreement**”), to provide certain educational or digital services to LEA.

WHEREAS, 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 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312).

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

NOW THEREFORE, in consideration of the mutual promises, covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which is acknowledged by the Parties, LEA and Provider hereby agree as follows:

1. The SDPC Standard Clauses, as attached hereto (the “**Standard Clauses**”), are fully incorporated into and made a part of this SDPA.
2. The following, only if checked, shall be fully incorporated into and made a part of this SDPA (collectively referred to herein as the “**Special Provisions**”):
 - ☐ Supplemental State Terms as set forth in **Exhibit “G”** attached to the Standard Clauses.
 - ☐ Additional terms or modifications set forth in **Exhibit “H”** attached to the Standard Clauses.
 - ☒ General Offer of Privacy Terms as set forth in **Exhibit “E”** attached to the Standard Clauses.
3. In the event of a conflict between the Standard Clauses and the Special Provisions, the terms of the Special Provisions will control. In the event there is conflict between the terms of the

SDPA and any other writing, including, but not limited to the Service Agreement and any terms of service or privacy policy of Provider, the terms of this SDPA shall control with respect to the subject matter of protecting Student Data.

4. A description of the services to be provided and the categories of student data that may be provided by LEA to Provider, and other information specific to this SDPA are contained in the Standard Clauses.
5. A description of the services to be provided by Provider to LEA pursuant to this SDPA are contained in **Exhibit “A”** to the Standard Clauses (the “**SDPA Services**”).
6. The term of this SDPA shall end upon the termination or expiration of the Service Agreement.
7. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below:

LEA-designated Representative:

As to FLVS: Florida Virtual School
Attn: Procurement and Contracting Department
5422 Carrier Drive, Suite 201
Orlando, FL 32819
Email: procurement@flvs.net

With a copy to: Florida Virtual School
Attn: General Counsel
5422 Carrier Drive, Suite 201
Orlando, FL 32819
Email: ogc@flvs.net

Provider-designated Representative:

Name: Deborah Fay
Title: Data Protection Officer
Address: 55 Almaden Blvd, San Jose, CA, 95113, Suite 600
Phone: +353 1 582 7141
Email: deborah.fay@zoom.us, with a copy to legal@zoom.us

Signature page follows on the next page

IN WITNESS WHEREOF, LEA and Provider have executed this SDPA on the dates set forth below.

Florida Virtual School

By: Louis J. Algaze, Ph.D. – President and CEO

Date: _____

Louis Algaze
Digitally signed by Louis
Algaze
Date: 2025.12.02
12:34:02 -05'00'

Attest: _____

Approved as to form:

**Karen M.
Chastain**
Digitally signed by Karen
M. Chastain
Date: 2025.11.19
09:13:19 -05'00'

FLVS Office of General Counsel

Zoom Communications, Inc.

By: _____

Name: _____

Date: _____

SDPC STANDARD CLAUSES

Version 1.0

Article I. **ARTICLE I: PURPOSE AND SCOPE**

1. **Purpose of SDPA.** The purpose of this SDPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations pertaining to Student Data, all as may be amended from time to time. In performing the SDPA Services, Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by LEA. Provider shall be under the direct control and supervision of LEA, with respect to its use of Student Data.
2. **Student Data to Be Provided.** In order to perform the SDPA Services, LEA shall provide to Provider certain Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **SDPA Definitions.** The definition of terms used in this SDPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this SDPA shall prevail over terms used in any other writing pertaining to the subject matter herein, including, but not limited to the Service Agreement and any terms of service or privacy policies of Provider.

Article II. **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data transmitted to Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of LEA. Provider further acknowledges and agrees that all copies of such Student Data transmitted to Provider, including any modifications or additions or any portion thereof (excluding De-Identified Data) from LEA or its authorized designee, are subject to the provisions of this SDPA in the same manner as the original Student Data. The Parties agree that as between them, all rights in and to Student Data, including all intellectual property rights therein, shall remain the exclusive property of LEA. For the purposes of FERPA, Provider shall be considered a School Official, under the control and direction of LEA as it pertains to the use of Student Data.
2. **Parent Access.** To the extent required by law, LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and Student Data and correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. To the extent the Provider has access to the data Provider shall respond in a reasonably timely manner (but no later than forty-five (45) days from the date of the request or the time frame required under state law for LEA to respond to a parent or student, whichever is sooner) to LEA’s request for Student Data in a student’s records held by Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts Provider to review any of the Student Data accessed pursuant to the Services, Provider shall refer the parent or individual to LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If Student-Generated Content is stored or maintained by Provider, then Provider shall, at the request of LEA, transfer, or provide a mechanism for LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities (each a “**Requesting Party**”) contact Provider with a request for Student Data held by Provider pursuant to the SDPA Services, Provider shall notify LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform LEA of the request, and any such notification to LEA will be in accordance with Provider’s government requests guide. LEA is on notice of and has reviewed Provider’s government requests guide located at <https://explore.zoom.us/en/trust/government-requests-guide/>, and LEA acknowledges that this SDPA does not restrict Provider’s right to modify the government requests guide from time to time.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for Provider in order for Provider to provide the Services (as defined in the Service Agreement), whereby each Subprocessor agrees to protect Student Data in a manner no less stringent than the terms of this SDPA. LEA is on notice of Provider’s Subprocessors listed [here](#), and LEA acknowledges that this SDPA does not restrict Provider’s right to modify it Subprocessors from time to time.

Article III. **ARTICLE III: DUTIES OF LEA**

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the SDPA Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If LEA has a policy of disclosing Education Records or Student Data under FERPA (34 CFR § 99.31(a)(1)), then 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. **Reasonable Precautions.** LEA shall protect Student Data by implementing administrative, physical, and technical safeguards, including those specifically designed to secure usernames, passwords, and any other means of gaining access to the SDPA Services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly and in all cases within seventy-two (72) hours of any known unauthorized access to Student Data or the SDPA Services. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.
5. **Use of Services and Consents.** LEA shall use the SDPA Services solely for educational purposes when using it with children under 13. LEA consents to Provider’s collection practices described in its Children’s Educational Privacy Statement located [here](#). LEA verifies that it is authorized to provide consent on behalf of its organization. LEA shall obtain any necessary parent or guardian consent for any third-party apps that LEA chooses to allow children to use in connection with the SDPA Services. LEA is on notice of Provider’s Privacy Statement [here](#) and the aforementioned Children’s Educational Privacy Statement, each of which LEA acknowledges and is aware of and consents to Provider’s right to modify these policies from time to time.

Article IV. **ARTICLE IV: DUTIES OF PROVIDER**

1. **Privacy Compliance.** Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security applicable to Provider in its performance of the SDPA Services, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than to deliver the SDPA Services outlined in **Exhibit “A”**, or stated in the Service Agreement, or otherwise authorized under the statutes referred herein. Provider will limit the use of, or access to, PII from Education Records of students to the limited scope of information actually needed to complete the Provider’s duties and/or Services under the Service Agreement. LEA has determined that Provider has a legitimate educational interest in receiving only the fields of Student Data in Exhibit B (for example, name, grade-level, school attending, etc.).
3. **Provider Employee Obligation.** Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this SDPA with respect to the Student Data shared as a result of Provider’s delivery of the SDPA Services to LEA. Provider agrees to require and maintain an employee nondisclosure agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider shall avoid, and shall instruct applicable employees/agents to avoid, accessing PII from Education Records of students, except for the legitimate purposes recognized under the Service Agreement, and shall require that all employees/agents accessing the data must be trained in the confidentiality requirements; and is under the direct control of LEA with respect to the use and maintenance of Education Records; and is subject to the requirements of 34 C.F.R. s. 99.33(a) governing the use and redisclosure of PII from an Education Record of a student, meaning the Provider may disclose PII from an Education Record only on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student as those terms are defined in 34 C.F.R. s. 99.3, and the officers, employees, and agents of a party that receive information from the Provider may use the information, subject to the limitations described above, but only for the purposes for which the disclosure was made; and shall not disclose or redisclose PII to a third party unless the disclosure is made pursuant to and authorized by: (a) FERPA and 34 CFR 99.31; or (b) prior written consent of a parent or an eligible student. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified Data, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing any work on behalf of Provider pursuant to this SDPA.
5. **De-Identified Data.** Provider agrees not to attempt to re-identify De-Identified Data. De-Identified Data may be used by Provider for those purposes allowed under FERPA and the following purposes: (1) assisting LEA or other governmental agencies in conducting research and other studies; and (2) research and development of Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the SDPA Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this SDPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer De-Identified Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Prior to publishing any document that names LEA explicitly or indirectly, Provider shall obtain LEA’s written approval of the manner in which De-Identified Data is presented.
6. **Disposition of Data.** Upon written request from LEA, Provider shall provide a mechanism for LEA to transfer Student Data obtained under the Service Agreement and held by Provider. If there is a written request from LEA, Provider will delete Student Data within sixty (60) days of

the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this SDPA and the Service Agreement, if no written request from LEA is received, Provider shall thereafter remove LEA access, dispose of all Student Data or both in accordance with Provider's practices, procedures, and data deletion policies. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Article II, Subsection 3. LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If LEA and Provider employ **Exhibit "D"**, then no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.

7. Provider shall comply with the requirements of the Family Educational Rights and Privacy Act (FERPA), its implementing regulations, Section 1002.22, Florida Statutes, the Protection of Pupil Rights Amendment (PPRA); the Student Online Personal Information Protection Act, F.S. 1006.1494 and implementing State Board of Education rules; and the Children's Online Privacy Protection Act (COPPA), 15 USC ss 6501-6506, and its implementing regulations, and shall not use any of the PII from Education Records of students that is received pursuant to the Agreement in violation of any applicable federal or state law, rule, or regulation. The PII must not be used for any other purpose other than the purposes outlined in this SDPA. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited. The Provider shall not share or sell a student's personally identifiable student information for commercial purposes, including but not limited to targeted advertising, without providing parents a means to consent or disapprove.
8. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the SDPA Services to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations) if the LEA affirmatively enables Zoom AI features; or (ii) to make product recommendations to third party teachers or LEA employees; or (iii) to notify the LEA about new education product updates, features, or services or from otherwise using Student Data as permitted in this SDPA and its accompanying exhibits.

Article V. **ARTICLE V: DATA PROVISIONS**

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States when US servers are selected by the LEA admin in the Provider's admin console. Upon request of LEA, Provider will provide a list of the locations where Student Data is stored. LEA acknowledges that certain Student Data may be disclosed or accessed outside the United States during a technical support engagement initiated by LEA. Additionally Provider will store and process PII from the Education Records of students in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards to secure PII from unauthorized access, disclosure, and use. Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Provider will also have a written incident response plan, to include prompt notification to LEA in the event of a security or privacy incident, as well as best practices for responding to a breach of PII. Provider agrees to share a summary of its incident response plan with LEA upon request. Provider shall maintain and revise its incident response plan to ensure that it is in a ready state at all times
2. **Audits.** No more than once a year, or following unauthorized access of Student Data, upon receipt of a written request from LEA with at least ten (10) business days' written notice and upon the execution of an appropriate confidentiality agreement, Provider shall allow LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or

any portion thereof as it pertains to the delivery of the SDPA Services to LEA. Provider will cooperate reasonably with LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of Provider or delivery of SDPA Services to students or LEA. The Provider will share its customer facing third party audit reports applicable to LEA upon written request from LEA on an annual basis. Provider may require additional terms of confidentiality as a condition to receipt of Provider's sensitive security-related information.

3. **Data Security.** Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. Provider and LEA shall adhere to any applicable law relating to data security. Provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Provider shall designate an employee to serve as LEA's primary contact regarding any data security concerns or questions.
4. **Data Breach.** In the event of a confirmed unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by Provider, Provider shall notify LEA in writing within seventy-two (72) hours of confirmation of the incident unless the timing of such notification would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of Student Data that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - iv. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all applicable federal and state requirements with respect to a data breach related to the Student Data.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and applicable federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
 - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

- (5) In the event of a breach originating from LEA's use of the SDPA Services, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

Article VI. **ARTICLE VI: GENERAL OFFER OF TERMS**

Intentionally deleted

Article VII. **MISCELLANEOUS**

1. **Termination**. In the event that either Party seeks to terminate this SDPA, they may do so by mutual written consent. Either party may terminate this SDPA and the Service Agreement if the other party materially breaches any terms of this SDPA and fails to cure the breach within thirty (30) days or another reasonable time agreed to by the parties in a duly signed writing.
2. **Effect of Termination and Survival**. If the Service Agreement and this SDPA are terminated, then Provider shall return or destroy all of LEA's Student Data in accordance with Provider's data deletion and destruction policies. Irrespective of termination of the Service Agreement and this SDPA, the obligations of Provider under this SDPA will continue until Provider has returned or destroyed all of the LEA's Student Data.
3. **Reserved**.
4. **Entire Agreement**. This SDPA constitutes 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 SDPA may be amended and the observance of any provision of this SDPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability**. Any provision of this SDPA 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 SDPA, 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, then it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this SDPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction**. THIS SDPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF FLORIDA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS IN THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SDPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound**: This SDPA is and shall be binding upon the respective successors and assigns of Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that

Provider sells, merges, or otherwise disposes of its business or assets to a successor during the term of this SDPA, Provider shall provide written notice to LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. LEA has the authority to terminate the SDPA if the LEA is prohibited from: (a) performing under this SDPA pursuant to a decision by a court or regulatory body of competent jurisdiction; or (b) contracting with the successor entity pursuant to applicable law. If LEA exercises its right to terminate this SDPA pursuant to sections (a) or (b) in the preceding sentence, then LEA must exercise such right within sixty (60) days of the event, otherwise the right to terminate will be automatically waived.

8. **Authority.** Each party represents that it is authorized to enter into this DPA and that the signatory is duly authorized to sign this DPA.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder 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

DESCRIPTION OF SERVICES

Please describe the functionality of the product and include if the application is a subscription or free online service. Also, include if the data is stored exclusively in the United States. If not, then list the countries in which data is stored.

<https://explore.zoom.us/en/services-description/>

Student Data is stored in the United States subject to LEA selecting US-only data centers in the administrative dashboard settings. LEA acknowledges that certain Student Data may be disclosed or accessed outside the United States during a technical support engagement initiated by LEA.

EXHIBIT B
SCHEDULE OF DATA – To be completed by the vendor

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X
	Other application technology meta data-Please specify: device type and features (such as camera version), technical product usage, settings (such as audio, video, screen sharing settings)	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications 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)	

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
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 (optional and only applicable if provided)	X
	Teacher names (optional and only applicable if provided)	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	

Category of Data	Elements	Check if Used by Your System
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (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 (optional and only applicable if provided)	X
Student work	Student generated content; writing, pictures, etc. (optional and only applicable if provided)	X

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application: profile picture if provided/optional	X

General	The categories of information in the privacy information, general information as provided in Provider's Privacy Statement (found here) and Provider's Children's Educational Privacy Statement (found here). This does not incorporate the terms from these documents into the SDPA.	X
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT C

DEFINITIONS

De-Identified Data and De-Identification: 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 individual or an individual's device.

Education Records: Education Records are defined by applicable law and, if not defined, are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

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.

Operator: means an Operator as defined by applicable law and, if not defined, an Operator means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "Operator" for the purposes of this section.

Originating LEA: An LEA who originally executes this SDPA in its entirety with Provider.

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.

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data, except to the extent expressly excluded under the definition of Metadata above. 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 SDPA, 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 Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student’s use of Provider’s services.

Subprocessor: For the purposes of this SDPA, the term “Subprocessor” means an entity that is not LEA or Provider, engaged by Provider to process Student Data on behalf of the LEA per the LEA’s instructions under the terms of this SDPA or the Service Agreement. Authorized Subprocessors may include Provider’s affiliates but shall exclude Provider employees, contractors and consultants.

Subscribing LEA: means an LEA who accepts Provider’s General Offer of Privacy Terms and is under a service agreement with Provider.

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 Operator's 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 any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

EXHIBIT D

DIRECTIVE FOR DISPOSITION OF DATA

LEA hereby directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider as follows:

1. Extent of Disposition

_____Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

Student and Staff Personally Identifiable Information

_____Disposition is Complete. Disposition extends to Personally Identifiable Information.

2. Nature of Disposition

_____Disposition shall be by destruction or deletion of data.

_____Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

Vendor will send a notification that the data destruction has been completed as described above.

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____As soon as commercially practicable.

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT E
Intentionally deleted

EXHIBIT F

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks 2/24/2020

The Education Security and Privacy Exchange (“**Edspex**”) works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* (“**Cybersecurity Frameworks**”) that may be utilized by Provider.

Cybersecurity Frameworks

MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
Center for Internet Security (CIS)	CIS Critical Security Controls (CSC, CIS Top 20)
Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

EXHIBIT G
SUPPLEMENTAL SDPC STATE TERMS FOR FLORIDA

Version _____

None

EXHIBIT H
ADDITIONAL TERMS OR MODIFICATIONS

None.