New York

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of last signature indicated below (the "**Effective Date**") and is entered into by and between: The Board of Cooperative Educational Services for the First Supervisory District, Erie County (the "**Local Education Agency**" or "**LEA**" or "**New York Original LEA**") and Zoom Communications Inc. (the "**Provider**").

WHEREAS, the Provider is providing video and voice communications and related information technology services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other educational 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), applicable state privacy laws and regulations and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. Provider agrees to offer the LEA all the same terms and conditions found in the Student Data Privacy Agreement between the Provider and Dedham Public Schools ("Originating LEA") which is dated October 7, 2023 ("Originating DPA"). The terms and conditions of the Originating DPA are thus incorporated herein.
2. Provider additionally agrees to the following additional terms outlined in the attached Exhibit "G" for New York, which will control in the event of a conflict between this DPA and the Originating DPA.
3. Provider may, by signing the attached form of "General Offer of Privacy Terms" be bound by the terms of the General Offer of Privacy Terms to any other LEA who signs the acceptance on said Offer. The form is limited by the terms and conditions described therein.
4. **Notices**. All notices or other communication required or permitted to be given pursuant to the Originating DPA may be given for the LEA via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Deborah Fay
Title: Data Protection Officer

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

The designated representative for the LEA for this DPA is:

Michelle Okal-Frink, Director of Instructional Technology, Research & Innovation
355 Harlem Road, West Seneca, NY 14224
Email: mokal@e1b.org
Phone: 716-821-7200

LEA: The Board of Cooperative Educational Services for the First Supervisory District, Erie County

By: James Fregelette
Date: 04/22/25

Printed Name: Jim Fregelette
Title/Position: Executive Director

Provider: Zoom Communications Inc.

By: Signed by: Deborah Fay
Date: Apr 17, 2025

Printed Name: Deborah Fay
Title/Position: Deputy General Counsel

DS
TS

Exhibit "G"

New York

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the Originating DPA.

3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security and Privacy Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security and Privacy Policy to the Provider upon execution of Exhibit "E". Provider shall have a thirty (30) day period to review each Subscribing LEA's Data Security and Privacy Policy to ensure Provider can comply with the requirements set forth therein. Should Provider determine that it cannot comply with a Subscribing LEA's Data Security and Privacy Policy, Provider will promptly notify the Subscribing LEA and may cancel the Exhibit E signed by the Subscribing LEA. Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.

4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider shall ensure that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the Service Agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all Providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under the Service Agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.

5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the Originating DPA to "Student Data" shall be amended to include and state, "Student Data and APPR Data."

7. To amend Article II, Section 6 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA's Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the data breach reporting requirements set forth in the DPA.

8. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider's employees and subprocessors who need to know the Student Data and APPR Data to provide the Services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such Services.

9. To replace Article IV, Section 6 (Disposition of Data) with the following: 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 ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider's certifying upon request by LEA that it and its subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.

   Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice, but in no event shall Provider retain Student Data beyond 90 days expiration or termination of the Service Agreement.

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 section II 3. The LEA may employ a "**Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D",** or, with reasonable notice to the Provider, other form of its choosing. 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".**

10. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."

11. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored which also can be found in LEA's admin portal.

12. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least thirty (30) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) 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 Services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's facilities (if such Access is required by law), staff, agents and LEA's Student Data and all records pertaining to the Provider's delivery of the Services to the LEA. The LEA may accept from Provider an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the LEA informed Provider that it required Provider to undergo an audit.

    Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed

Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

13. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit 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 the 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 personal information 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.

    iv. 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

    v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

    vi. The number of records affected, if known; and

    vii. A description of the investigation undertaken so far; and

    viii. The name of a point of contact for Provider.

    (2) Provider agrees to adhere to all applicable federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

    (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and 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. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly

reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.

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

(6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

14. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the Provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its Service, and who has access to Student Data.

- "Provider" is also known as a third party contractor. It is any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit "C" the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration,

including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.

- **Disclose or Disclosure**: The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District**: As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

Exhibit "J"

LEA Documents

LEA's Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy for this service agreement can be accessed at:

https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=13045

Exhibit "K"

Provider Security Policy

Provider's Data Security and Privacy Plan can be accessed at https://explore.zoom.us/en/trust/.

Erie 1 BOCES DPA Signed by Zoom

Final Audit Report 2025-04-22

Created:	2025-04-22
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAAZs982irilIUboU7WjG76MidMvwzyfja

"Erie 1 BOCES DPA Signed by Zoom" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2025-04-22 - 4:58:32 PM GMT

Document emailed to James Fregelette (jfregelette@e1b.org) for signature
2025-04-22 - 4:58:36 PM GMT

Email viewed by James Fregelette (jfregelette@e1b.org)
2025-04-22 - 6:03:55 PM GMT

Document e-signed by James Fregelette (jfregelette@e1b.org)
Signature Date: 2025-04-22 - 6:04:53 PM GMT - Time Source: server

Agreement completed.
2025-04-22 - 6:04:53 PM GMT

STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, NEW HAMPSHIRE, RHODE ISLAND, AND VERMONT

MA-ME-NH-RI-VT-DPA, Modified Version 1.0

DEDHAM PUBLIC SCHOOLS

and

ZOOM VIDEO COMMUNICATIONS, INC.

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of the last signature indicated below (the "**Effective Date**") and is entered into by and between: Dedham Public Schools, located at 100 Whiting Avenue, Dedham, MA 02026 (the "**Local Education Agency**" or "**LEA**") and Zoom Video Communications, Inc., located at 55 Almaden Blvd, Suite 600, San Jose, CA 95113 ("**Zoom**" or the "**Provider**").

WHEREAS, the Provider is providing video and voice communications and related information technology services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect Student Data and other educational 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), applicable state privacy laws and regulations and

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

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

1. A description of the Services (as defined in Section 5 below) to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **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.

   ☑ If checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms.

3. **Conflict Resolution**. In the event of a conflict between any parts of or exhibits to this DPA, the following order of precedence will apply: (i) Supplemental State Terms; (ii) Standard Clauses Articles I-VII; and (iii) other parts, sections, or exhibits to this DPA. In the event there is conflict between the terms of this DPA and any other writing pertaining to the subject matter herein, including, but not limited to the service agreement or Provider terms of service ("**Service Agreement**"), the Provider's Privacy Statement, and the Provider's Children's Educational Privacy Statement (collectively "Provider Terms" herein) the terms of this DPA shall govern and control to the extent required to resolve the conflict. Nothing in this DPA may be relied upon to modify or change any applicable limitations on liability or defense or indemnity obligations under the Service Agreement. The "Consent to Educational Data Collection Practices" ("Consent") issued by Provider will not modify the terms of this DPA. The parties intend for this DPA to be a separate contractual agreement that is not superseded or modified by any such Consent. No future consent or acknowledgement will supersede or modify the terms of the DPA absent an express signed agreement between LEA and Provider to the contrary.

4. This DPA shall stay in effect for three years from the Effective Date. Exhibit E will be coterminous with this DPA and shall expire 3 years from the Effective Date of this DPA.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A,"** unless separate terms are currently in effect between the parties pursuant to the Service Agreement (the "**Services**"). All obligations under this DPA apply only to Zoom Services.

6. **Notices**. 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.

The designated representative for the Provider for this DPA is:

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_____

The designated representative for the LEA for this DPA is:

Technology Director
Dedham Public Schools
100 Whiting Avenue, Dedham, MA 02026
(781) 310-1000
dlangenhorst@dedham.k12.ma.us

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

DEDHAM PUBLIC SCHOOLS

By: Don Langenhorst, EdD
Don Langenhorst, EdD (Oct 7, 2023 10:36 EDT)

Date: 10/7/2023

Printed Name: Don Langenhorst, EdD

Title/Position: Technology Director

ZOOM VIDEO COMMUNICATIONS, INC.

DS TS

By: DocuSigned by: Deborah Fay
AA444A874F98427...

Date: Oct 5, 2023

Printed Name: Deborah Fay

Title/Position: Deputy General Counsel

STANDARD CLAUSES
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data, including commitments to comply 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 Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing Services that would otherwise be provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to Provider's use of Student Data.

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Type of Data, attached hereto as **Exhibit "B"**.

3. **DPA Definitions**. Defined terms used in this DPA are located in the relevant section or can be found in **Exhibit "C."** Defined terms are identified by the use of a capitalized first letter**.** In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing pertaining to the subject matter herein, including, but not limited to, the Provider Terms.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. Student Data Property of LEA. All Student Data transmitted to the Provider pursuant to the Provider Terms is and will continue to be the property of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider by LEA, 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 DPA in the same manner as the original Student Data. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data.

2. Parent Access. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data, correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of the Services. If a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. LEA Student Data Access. Provider shall retain Student Data and LEA shall have access to such Student Data for 15 months following its collection. Provider shall offer reasonable means for LEA to download or transfer such Student Data throughout this time. Upon termination, Student Data will only be accessible for the time periods set forth in Provider's Service Agreement.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("**Requesting Party(ies)**") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA to the extent allowed by law and in accordance with Provider's government requests guide. LEA is on notice of and has reviewed Provider's government requests guide

currently located at https://explore.zoom.us/en/trust/government-requests-guide/, and LEA acknowledges that this DPA does not restrict Provider's right to modify the government requests guide from time to time. No future modification of the government requests guide will supersede or modify the terms of this DPA if it conflicts with the DPA absent an express signed agreement between LEA and Provider to the contrary.

5. **Public Records Requests.** LEA is responsible for responding to all public records requests, and Provider is under no obligation to gather, retrieve, recreate, or otherwise use its personnel to respond to a public records request, except as required by law or at Provider's sole discretion.

6. Subprocessors. Provider shall enter into written agreements 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 are reviewed for appropriate administrative, technical, and physical safeguards that are appropriate for the services being performed and the data being processed and that they protect Student Data consistent with this DPA. LEA is on notice of Provider's subprocessors listed here, and LEA acknowledges that this DPA does not restrict Provider's right to modify it subprocessors from time to time consistent with its obligations under this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall share and provide Student Data only for the purposes of obtaining the 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 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. **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 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 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 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 as of the date of execution except the following: (1) Student Data may not be used for product research and development; (2) Student Data will not be disclosed for security or safety reasons unless required by law, as set forth in Article II, Section 4 above (Law Enforcement Requests), or there is imminent danger of death or serious physical injury, which means that death or serious physical injury could occur within a short time if no intervention is immediately initiated. (3) the LEA does not need to obtain parent or guardian consent to the third-party app's data practices should the third-party app be used for educational purposes. LEA verifies that it is authorized to provide consent on behalf of its organization. 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. However, any future modification of the Children's Educational Privacy Statement is not automatically incorporated herein. The parties intend for this DPA to be a separate contractual agreement that is not superseded or modified by any future change to the Children's Educational Privacy Statement. No future modification of the Children's Educational Privacy Statement will supersede or modify the terms of the DPA if it conflicts with the DPA absent an express signed agreement between LEA and Provider to the contrary.

ARTICLE IV: DUTIES OF PROVIDER

1. Privacy Compliance. The Provider shall comply with all of its obligations, including as a School Official, under applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security 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 (i) to deliver the Services, (ii) as stated in the Provider Terms and (iii) as otherwise permitted by law. Notwithstanding the prior sentence, the Provider agrees that it will not disclose any Student Data except in accordance with Article IV, Section 4, irrespective of what is permitted by law or what is outlined in the Provider's Terms.

3. Provider Employee Obligation. Provider agrees to require that all employees with access to Student Data pursuant to the Service Agreement be bound by an employee non-disclosure agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data other than as directed or permitted by the LEA, this DPA, or as required by applicable law. This prohibition against disclosure shall not apply to: (a) aggregate summaries of De-Identified Data, (b) Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or (c) subprocessors, subcontractors, or Provider affiliates performing services on behalf of the Provider. Provider will not sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purposes and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA 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 the LEA who has provided prior written consent for such transfer. This prior sentence does not apply to aggregate summaries of De-Identified Data in accordance with Article IV, Section 4. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.

6. Disposition of Data. Upon written request from the LEA, Provider shall provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement during the term of the Service Agreement and for a period of thirty (30) days following termination or expiration of the Service Agreement. If there is a written request from the LEA, the Provider will delete Student Data within sixty days of the request. . Upon termination of this DPA and the Service Agreement, if no written request from the 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.

7. 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 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); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. LEA acknowledges that certain Student Data may be disclosed or accessed outside the United States during a technical support engagement initiated by LEA.

2. **Audits.** No more than once a year, or following unauthorized access of Student Data, upon receipt of a written request from the LEA with at least ten (10) business days' prior written notice, the Provider will allow the LEA to audit the security and privacy policies that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of Services to the 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. The Provider will cooperate reasonably with the LEA and any state, or federal agency with oversight authority or jurisdiction in connection with any state or federal audit or investigation of the Provider and/or delivery of Services to students and/or LEA

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 and LEA shall adhere to applicable law relating to data security. The Provider shall implement reasonable technical and organizational data security measures which are aligned with one of the CyberSecurity Frameworks in **Exhibit "F"**.

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 the Provider, the Provider shall provide email notification to LEA within seventy-two (72) hours of confirmation of the unauthorized release, disclosure or acquisition. In such an event, notification shall be made within a reasonable time after the incident. For clarity, Provider's obligations of notice under this Section 4 (Data Breach) are limited to unauthorized access to or exfiltration of Student Data. 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 the 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; and
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.
iv. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Provider further acknowledges and agrees to have a written incident response plan and agrees to provide LEA, upon request, with a customer-facing summary of said written incident response plan.

(3) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(4) In the event of a breach originating from LEA's use of the Services, Provider shall reasonably cooperate with LEA to assist LEA in its efforts to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS

Provider agrees, by signing the attached form of "General Offer of Privacy Terms" (attached hereto as Exhibit "E"), to be bound by the terms of this DPA and Exhibit "E" with any Subscribing LEA who countersigns on said Exhibit E. Any applicable Exhibit "G" Supplemental State Terms must be attached to each Exhibit "E" General Offer of Privacy Terms at the time of execution of Exhibit E. If there is an amendment to this DPA that applies to the LEA, the The Education Cooperative will provide written notice to any Subscribing LEA of that amendment. A Subscribing LEA agrees that if it does not object to the amendment within thirty (30) days of receipt of notice of the amendment, the right to object will be automatically waived and the Subscribing LEA will be bound to the amendment. If the Subscribing LEA objects to the amendment, the parties will work in good faith to reach resolution. Unless the amendment is required by law, if the parties cannot reach resolution, the Subscribing LEA may terminate the DPA and Service Agreement.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent. Either party may terminate this DPA and any affected portion of the Service Agreement if the other party materially breaches any terms of this DPA 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 DPA are terminated, the 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 DPA, the obligations of Provider under this DPA will continue until Provider has returned or destroyed all of the LEA's Student Data.

3. **Counterparts and Electronic Signatures**. This DPA and any Exhibit hereto may be executed in one or more counterparts. Each counterpart will be an original, but all such counterparts will constitute a single instrument. This DPA and any Exhibit hereto may be electronically or digitally signed, and any electronic or digital signatures appearing on this DPA or an Exhibit are the same as handwritten signatures for the purposes of validity, enforceability, and admissibility.

4. **Entire Agreement; Modifications; Waiver**. This DPA 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 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. 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 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.

6. **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. IN THE EVENT OF A DISPUTE THAT INVOLVES BOTH THE PROVIDER TERMS AND THIS DPA, THEN THE GOVERNING LAW AND VENUE SET FORTH IN THE SERVICES AGREEMENT WILL GOVERN AND CONTROL.

7. **Successors and Assigns**: This DPA is and shall be binding upon the respective successors and assigns of the parties, whether through merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business or assets to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. In the event that the Provider sells, merges, or otherwise disposes of its business or assets to a successor during the term of this DPA, then the LEA may terminate this DPA if the LEA is prohibited from: (a) performing under this DPA 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 DPA 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 the terms of this DPA and that its signatory is duly authorized to sign this DPA.

EXHIBIT "A"

DESCRIPTION OF SERVICES

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

EXHIBIT "B"

SCHEDULE OF TYPE OF DATA AND PROCESSING DETAILS

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 (e.g. video recordings, chats)	**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-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	

Category of Data	Elements	Check if Used by Your System
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 and meeting host names (optional and only applicable if provided)	**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-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 (optional and only applicable if provided)	**X**
	Student app passwords (optional and only applicable if provided)	**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 during Zoom meeting)	**X**

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	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 transportation data – Please specify:	

Category of Data	Elements	Check if Used by Your System
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 DPA.	**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 mean 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: mean Education Records defined by applicable law and, if not defined, Education Records 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 (as defined under applicable law).

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 means an LEA who originally executes this DPA in its entirety with the Provider.

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: means for the purposes of this DPA and pursuant to 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 its own employees; (2) via this DPA is 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 means 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 may include Metadata, 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 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 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 DPA, 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 DPA or the Service Agreement. Authorized Subprocessors may include Zoom Affiliates but shall exclude Zoom employees, contractors and consultants.

Subscribing LEA: means an LEA who accepts the Provider's General Offer of Privacy Terms, is under a Service Agreement with Provider, and is authorized by Zoom and The Education Cooperative Student Data Privacy Alliance.

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"

If there is a written request from the LEA, the Provider will delete Student Data within sixty (60) days of the request. Otherwise, the Provider will delete and destroy Student Data in accordance with Provider's data deletion policy.

EXHIBIT "F"

As of the Effective Date, Zoom materially adheres to and is audited against at least the following security baselines and standards: ISO/IEC 27001:2013, and AICPA System and Organization Controls (SOC) 2, Type 2.

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
3. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
4. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
5. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
6. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
    a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
    b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
    c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT "G"

Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
3. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
4. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
5. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:

    i. **Information about what the Provider has done to protect individuals whose information has been breached,** including toll free numbers and websites to contact:

        1. The credit reporting agencies
        2. Remediation service providers
        3. The attorney general

    ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

    iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible students requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT "G"
Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.
Date of birth.
Personal street address.
Personal email address.
Personal telephone number
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

Notwithstanding the foregoing, the parties agree that if an individual student or teacher forms a direct relationship with Zoom outside of K-12 school purposes, neither this DPA nor its restrictions will apply to that individual student or teacher data.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I".**
3. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,…"
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

6. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:

(1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;

(2) Limit unsuccessful logon attempts;

(3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;

(4) Authorize wireless access prior to allowing such connections;

(5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

(6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

(7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;

(8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

(9) Enforce a minimum password complexity and change of characters when new passwords are created;

(10) Perform maintenance on organizational systems;

(11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;

(12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;

(13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;

(14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

(15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;

(16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

(17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

(18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

(19) Protect the confidentiality of Student Data and Teacher Data at rest;

(20) Identify, report, and correct system flaws in a timely manner;

(21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

(22) Monitor system security alerts and advisories and take action in response; and

(23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

7. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
    i. The estimated number of students and teachers affected by the breach, if known.
8. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
9. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER DATA		
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
Communications	Online communications that are captured (e.g. video recordings, chats; email communication optional and only applicable if optional email service is used)	X
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses (optional and only applicable if provided)	X
	Teacher calendar (optional and only applicable if provided)	X
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	X
	Teacher app username	X
	Teacher app passwords	X
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires (optional and only applicable as provided)	X
Teacher work	Teacher generated content; writing, pictures etc. (optional and only applicable as provided)	X
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application: profile pic if provided/optional	X

Zoom_Dedham_VendorSigned

Final Audit Report 2023-10-07

Created:	2023-10-07
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAL4se7fZr_GHS0LL3RzCrtkOxjbQovEvI

"Zoom_Dedham_VendorSigned" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2023-10-07 - 12:55:55 PM GMT- IP address: 108.35.203.7

Document emailed to Don Langenhorst (dlangenhorst@dedham.k12.ma.us) for signature
2023-10-07 - 12:57:20 PM GMT

Email viewed by Don Langenhorst (dlangenhorst@dedham.k12.ma.us)
2023-10-07 - 2:35:27 PM GMT- IP address: 96.230.87.138

Signer Don Langenhorst (dlangenhorst@dedham.k12.ma.us) entered name at signing as Don Langenhorst, EdD
2023-10-07 - 2:36:28 PM GMT- IP address: 96.230.87.138

Document e-signed by Don Langenhorst, EdD (dlangenhorst@dedham.k12.ma.us)
Signature Date: 2023-10-07 - 2:36:30 PM GMT - Time Source: server- IP address: 96.230.87.138

Agreement completed.
2023-10-07 - 2:36:30 PM GMT