STUDENT DATA PRIVACY AGREEMENT

MAINE AND VERMONT

MA-VT-DPA, Modified Version 1.0

CHAMPLAIN VALLEY SCHOOL DISTRICT

and

FLIPGRID, INC.

This Student Data Privacy Agreement ("DPA") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Champlain Valley School District, located at 5420 Shelburne Road, Shelburne, VT 05482 (the "Local Education Agency" or "**LEA**") and Flipgrid, Inc., located at One Microsoft Way, Redmond, WA 98052-6399") (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.
WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 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 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 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 and 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. In the event of a conflict between the SDPC Standard Clauses, and the Special Provisions, the Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for one year from the Effective Date (the "Initial Term"), after which this DPA will renew for consecutive one year periods (each, a "Renewal Term", with the Initial Term and each Renewal Term together forming the "Term"), unless the parties amend the Term by mutual written agreement or Provider gives three months written notice prior to the start of a Renewal Term of its intent to replace this DPA with another agreement addressing the same subject matter as this DPA. Notwithstanding the foregoing, until this DPA is replaced by another agreement addressing the subject matter of this DPA, the Provider shall be bound by this DPA for so long as the Provider maintains any Student Data collected via the Services.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**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: ____Deb McFadden____________________Title: ____General Manager of Flip_____________________

Address: ___One Microsoft Way, Redmond, WA 98052____________________________________

Phone: ____________________________

Email: ___flipsupport@microsoft.com__________________________________

The designated representative for the LEA for this DPA is:

Bonnie Birdsall, Director of Digital Learning & Communication
Champlain Valley School District
5420 Shelburne Rd, Shelburne, VT 05482
802-383-1234
bbirdsall@cvsdvt.org

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

CHAMPLAIN VALLEY SCHOOL DISTRICT

By: Bonnie Birdsall
Bonnie Birdsall (May 5, 2023 15:08 EDT)_________________________________

Date: May 5, 2023

Printed Name: Bonnie Birdsall

Title/Position: Director of Digital Learning and Communication

FLIPGRID, INC.

By: Deb McFadden
____

Date: ___04/18/2023_________________

Printed Name: _____ Deb McFadden ________________________________

Title/Position: _________ General Manager of Flip ___________________________________

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 compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Nature of Services Provided**. The Provider has agreed to provide the Services to the LEA and any individual educator who has signed-up for the Services pursuant to the LEA's policies and processes using an LEA Issued Email Address ("LEA Educator"). The LEA agrees that such LEA Educators are authorized agents of the LEA.

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

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. 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, notwithstanding the above. The LEA may access, download and delete Student Data through the LEA Educator account associated with the Group to which such Student Data was submitted. The Provider will reasonably cooperate with any other request regarding Student Data made by the LEA within ten (10) days of the LEA's request. Students may access and download their Student Data maintained by the Provider by going to my.flipgrid.com.

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 services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that 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. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA reasonably cooperate with LEA in transferring, or providing a mechanism for the LEA to transfer, said Student-Generated Content to a separate school account created by the student.

4. **Law Enforcement and other Third Party Requests**. Should a Third Party, including, but not limited to law enforcement, former employees of the LEA (including former LEA educators whose email address is associated with the Flipgrid account), current employees of the LEA, and government entities, contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall make reasonable efforts to redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited.

5. **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 agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data 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 take reasonable precautions 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 of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all 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 the Services outlined in Exhibit A or stated in the Service Agreement, this DPA and/or otherwise authorized under the statutes referred to herein this DPA.

3. **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 DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. 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 purpose 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 that party agrees in writing not to attempt re-identification and to the use restrictions of De-Identified Data specified in this DPA. 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 the LEA is named explicitly or indirectly.

6. **Disposition of Data**. Upon written request from the LEA Educator account, Provider shall dispose of Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. 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 reasonable prior notice. 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, Section 3. The LEA may email flipsupport@microsoft.com from the email address associated with a particular LEA Educator account to request closure of an LEA Educator account or deletion any Student Records associated with an LEA Educator account. Students or LEA may access and export all Student Data available through my.flipgrid.com as described in Article II, Section 1 of this DPA.

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 Service 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.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will provide the LEA with a Provider Audit Report, defined below. Provider will conduct audits of the security of the computers, computing environment and physical data centers that is uses in processing Student Records, where each audit will be performed (i) according to the standards and rules of the regulatory or accreditation body for any applicable control standard or framework consistent with industry standards, and (ii) by qualified, independent, third party security auditors at Provider's selection and expense. Each audit will result in the generation of an audit report ("**Provider Audit Report**"), which will be Provider's confidential information and will clearly disclose any material findings by the auditor. Provider will promptly remediate issues raised as critical by the auditor in the Provider Audit Report to the satisfaction of the auditor. The Provider will reasonably cooperate with the LEA and any local, state or federal agency with oversight authority or jurisdiction in connection with any legally required audit or investigation of the LEA's use of Services to students and/or LEA.

3. **Data Security**. The Provider agrees to utilize reasonable administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**.

4. **Data Breach**. In the event of an 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 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. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

      i. 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.

      ii. 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

      iii. 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, 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 any 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 respond to inquiries emailed to flipsupport@microsoft.com at reasonable times to answer the LEA's questions on the written incident 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 Service, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data.

(6) LEA is solely responsible for complying with its obligations under incident notification laws applicable to LEA and fulfilling the LEA's third-party notification obligations related to any breach of Student Data.

(7) Provider's cooperation with LEA in connection with a breach of Student Data is not an acknowledgement by Provider of any fault or liability with respect to the breach of Student Data.

(8) LEA must notify Provider promptly about any possible misuse of LEA Educator accounts or authentication credentials or any security incident related to the Services.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. Except as otherwise provided herein, in the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA. The LEA may terminate this DPA at any time by ceasing to use the Services.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, LEA may close LEA Educator accounts and require the Provider to destroy Student Data associated with that LEA Educator account in accordance with Article IV, section 6.

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including, as applicable, those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service

Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses, and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

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

7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to 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 the Provider sells, merges, or otherwise disposes of its business 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. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

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

Flip is the leading video-discussion platform used by K12-PhD educators all over the world.

Through Flip’s platform on the Flip.com website, the Flip mobile app, and any associated

services (collectively, the “Services”), students are invited to contribute video and comments to a “Grid” created and managed by educators for their classroom community. Grids operate by having educators create discussion “Topics” on their Grid anytime they want to start a conversation and inviting students to respond by recording short videos. Grid participants generally have access permissions to view and comment on videos submitted to a Grid and certain Grid content may be shared outside the Grid by the educator.

EXHIBIT “B”

SCHEDULE OF 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 OS, Browser OS, Anonymized diagnostic data
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	X – educators may provide feedback to students
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
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:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	

Category of Data	Elements	Check if Used by Your System
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
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:	
Category of Data	**Elements**	**Check if used by your system**
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	
	Student app passwords	
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	
Student work	Student generated content; writing, pictures etc.	X
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	

Category of Data	Elements	Check if Used by Your System
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	
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, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information. For clarity, De-Identified Data is not Student Data.

Educational Records: Educational 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.

LEA Educator: Any individual educator who has signed-up for the Services using an email address issued by the LEA. LEA Educators are authorized agents of the LEA.

LEA Issued Email Address: Any email address using the following domain(s): @cvsdvt.org or any domain(s) designated by a Subscribing Provider pursuant to Exhibit "E".

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.

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 the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

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 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 employees; (2) 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.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

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. 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" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

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.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT “D”

DIRECTIVE FOR DISPOSITION OF DATA

[**Insert Name of District or LEA**] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

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:

[**Insert categories of data here**]

_____ Disposition is Complete. Disposition extends to all categories of data.

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:

[**Insert or attach special instructions**]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By [**Insert Date**]

4. Signature

____ ____________________

Authorized Representative of LEA Date

5. Verification of Disposition of Data

____ _______________

Authorized Representative of Company Date

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)**
x	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	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 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.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

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. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct unmonitored contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont 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. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct unmonitored contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. 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.
6. 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.
7. 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.

DPA - CHAMPLAIN VALLEY SCHOOL DISTRICT and FLIPGRID - FINAL

Interim Agreement Report 2023-04-26

Created:	2023-04-18
By:	Flip Agreements (flipagreements@microsoft.com)
Status:	Out for Signature
Transaction ID:	CBJCHBCAABAAuHweZ4I5CHpb_Gyt32BXRBJGGXKXU8yw

Agreement History

Agreement history is the list of the events that have impacted the status of the agreement prior to the final signature. A final audit report will be generated when the agreement is complete.

"DPA - CHAMPLAIN VALLEY SCHOOL DISTRICT and FLIPGRID - FINAL" History

Document created by Flip Agreements (flipagreements@microsoft.com)
2023-04-18 - 2:05:45 AM GMT

Document emailed to Deb McFadden (Deb.McFadden@microsoft.com) for signature
2023-04-18 - 2:15:59 AM GMT

Email viewed by Deb McFadden (Deb.McFadden@microsoft.com)
2023-04-18 - 2:28:47 AM GMT

Email viewed by Deb McFadden (Deb.McFadden@microsoft.com)
2023-04-25 - 7:46:12 AM GMT

Document e-signed by Deb McFadden (Deb.McFadden@microsoft.com)
Signature Date: 2023-04-25 - 4:07:04 PM GMT - Time Source: server

Document emailed to jhawley@tec-coop.org for signature
2023-04-25 - 4:07:06 PM GMT

Email viewed by jhawley@tec-coop.org
2023-04-26 - 3:11:48 AM GMT

DPA - CHAMPLAIN VALLEY SCHOOL DISTRICT and FLIPGRID - FINAL

Final Audit Report 2023-04-28

Created:	2023-04-28
By:	Flip Agreements (flipagreements@microsoft.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAuQZNB1TIqms_AWBOb6c3psSSq0scb5Tq

"DPA - CHAMPLAIN VALLEY SCHOOL DISTRICT and FLIPGRID - FINAL" History

Document created by Flip Agreements (flipagreements@microsoft.com)
2023-04-28 - 7:22:11 PM GMT

Document emailed to Deb McFadden (Deb.McFadden@microsoft.com) for signature
2023-04-28 - 7:23:14 PM GMT

Email viewed by Deb McFadden (Deb.McFadden@microsoft.com)
2023-04-28 - 7:37:38 PM GMT

Document e-signed by Deb McFadden (Deb.McFadden@microsoft.com)
Signature Date: 2023-04-28 - 7:38:43 PM GMT - Time Source: server

Agreement completed.
2023-04-28 - 7:38:43 PM GMT

Flip_Champlain_VendorSigned

Final Audit Report 2023-05-05

Created:	2023-05-05
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAATjBp-xFBuHoODda3ZJ94otuTh6sJzLos

"Flip_Champlain_VendorSigned" History

Document created by Ramah Hawley (rhawley@tec-coop.org)

2023-05-05 - 7:06:23 PM GMT- IP address: 100.1.89.97

Document emailed to bbirdsall@cvsdvt.org for signature

2023-05-05 - 7:06:57 PM GMT

Email viewed by bbirdsall@cvsdvt.org

2023-05-05 - 7:07:27 PM GMT- IP address: 64.25.209.77

Signer bbirdsall@cvsdvt.org entered name at signing as Bonnie Birdsall

2023-05-05 - 7:07:58 PM GMT- IP address: 64.25.209.77

Document e-signed by Bonnie Birdsall (bbirdsall@cvsdvt.org)

Signature Date: 2023-05-05 - 7:08:00 PM GMT - Time Source: server- IP address: 64.25.209.77

✓ Agreement completed.

2023-05-05 - 7:08:00 PM GMT

This Student Data Privacy Agreement (“DPA”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Champlain Valley School District, located at 5420 Shelburne Road, Shelburne, VT 05482 (the “Local Education Agency” or “**LEA**”) and Flipgrid, Inc., located at One Microsoft Way, Redmond, WA 98052-6399”) (the “**Provider**”).

~~____ (the “**Provider**”).~~

WHEREAS**,** the Provider is providing educational or digital services to LEA.

WHEREAS**,** the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 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 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 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 and 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. In the event of a conflict between the SDPC Standard Clauses, and the ~~State or~~Special Provisions, the Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for ~~three years. Exhibit E will expire 3 years from the date the original DPA was signed.~~one year from the Effective Date (the “Initial Term”), after which this DPA will renew for consecutive one year periods (each, a “Renewal Term”, with the Initial Term and each Renewal Term together forming the “Term”), unless the parties amend the Term by mutual written agreement or Provider gives three months written notice prior to the start of a Renewal Term of its intent to replace this DPA with another agreement addressing the same subject matter as this DPA. Notwithstanding the foregoing, until this DPA is replaced by another agreement addressing the subject matter of this DPA, the Provider shall be bound by this DPA for so long as the Provider maintains any Student Data collected via the Services.

Title/Position: ____

FLIPGRID, INC.

By: ____

Date: _____________________

Printed Name: ____

Title/Position: ____

STANDARD CLAUSES

Version 1.0

ARTICLE I: PURPOSE AND SCOPE

~~2.~~1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Nature of Services Provided**. The Provider has agreed to provide the Services to the LEA and any individual educator who has signed-up for the Services pursuant to the LEA's policies and processes using an LEA Issued Email Address ("LEA Educator"). The LEA agrees that such LEA Educators are authorized agents of the LEA.

~~3.~~ 3. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as Exhibit "B".

~~5.~~ 4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

~~2.~~ 1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. 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, notwithstanding the above. The LEA may access, download and delete Student Data through the LEA Educator account associated with the Group to which such Student Data was submitted. The Provider will reasonably cooperate with any other request regarding Student Data made by the LEA within ten (10) days of the LEA's request. Students may access and download their Student Data maintained by the Provider by going to my.flipgrid.com.

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 services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that 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. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA~~, transfer~~ reasonably cooperate with LEA in transferring, or ~~provide~~providing a mechanism for the LEA to transfer, said Student-Generated Content to a separate school account created by the student.

4. **Law Enforcement and other Third Party Requests**. Should a Third Party, including, but not limited to law enforcement~~ or other~~, former employees of the LEA (including former LEA educators whose email address is associated with the Flipgrid account), current employees of the LEA, and government entities ~~("Requesting Party(ies)")~~, contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall make reasonable efforts to redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required

information. Provider shall notify the LEA in advance of a compelled disclosure to ~~the Requesting~~a Third Party, unless ~~lawfully directed by the Requesting Party not to inform the LEA of the request~~legally prohibited.

5. **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 agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

~~2.~~1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data 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.

~~4.~~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.

~~6.~~3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

~~8.~~4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

~~2.~~1. **Privacy Compliance**. The Provider shall comply with all 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.

~~4.~~2. Authorized Use. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service ~~Agreement and~~Agreement, this DPA and/or otherwise authorized under the statutes referred to herein this DPA.

~~6.~~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 DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

~~8.~~4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

~~10.~~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 purpose 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 Student~~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.~~ use restrictions of De-Identified Data specified in this DPA. 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.~~the LEA is named explicitly or indirectly.

~~12.~~6. **Disposition of Data**. Upon written request from the LEA Educator account, Provider shall dispose of ~~or provide a mechanism for the LEA to transfer~~ Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. 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 reasonable prior notice. 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”**. If the LEA and Provider employ Exhibit “D,” 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.~~The LEA may email support@flipgrid.com from the email address associated with a particular LEA Educator account to request closure of an LEA Educator account or deletion any Student Records associated with an LEA Educator account. Students or LEA may access and export all Student Data available through my.flipgrid.com as described in Article II, Section 1 of this DPA

~~14.~~ 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 Service 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

~~2.~~1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. ~~Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.~~

~~3.~~2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will ~~allow~~provide the LEA ~~to audit~~ with a Provider Audit Report, defined below. Provider will conduct audits of the security of the computers, computing environment and ~~privacy measures~~physical data centers that ~~are~~is uses in ~~place to ensure protection of~~ processing Student ~~Data~~Records, where each audit will be performed (i) according to the standards and rules of the regulatory or accreditation body for any ~~portion thereof~~applicable control standard or framework consistent with industry standards, and (ii) by qualified, independent, third party security auditors at Provider's selection and expense. Each audit will result in the generation of an audit report ("**Provider Audit Report**"), which will be Provider's confidential information and will clearly disclose any material findings by the auditor. Provider will promptly remediate issues raised as ~~it pertains to the delivery of services to the LEA .~~critical by the auditor in the Provider Audit Report to the satisfaction of the auditor. The Provider will ~~cooperate~~ reasonably cooperate with the LEA and any local, state~~,~~ or federal agency with oversight authority or jurisdiction in connection with any legally required audit or investigation of the ~~Provider and/or delivery~~LEA's use of Services to students and/or LEA~~, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.~~.

~~4.~~3. **Data Security**. The Provider agrees to utilize reasonable administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**.

~~Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.~~

~~5.~~4. **Data Breach**. In the event of an 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 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.~~i. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

~~iii.~~i. 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.~~ii. 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.~~iii. 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, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

~~(4)~~(3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and any 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~~respond to inquiries emailed to support@flipgrid.com at reasonable times to answer the LEA's questions on the written incident ~~response~~ plan.

~~(6)~~(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

~~(8)~~(5) In the event of a breach originating from LEA's use of the Service, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data.

(6) LEA is solely responsible for complying with its obligations under incident notification laws applicable to LEA and fulfilling the LEA’s third-party notification obligations related to any breach of Student Data.

(7) Provider’s cooperation with LEA in connection with a breach of Student Data is not an acknowledgement by Provider of any fault or liability with respect to the breach of Student Data.

(8) LEA must notify Provider promptly about any possible misuse of LEA Educator accounts or authentication credentials or any security incident related to the Services.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of “General Offer of Privacy Terms” (General Offer, attached hereto as **Exhibit “E”**), be bound by the terms of **Exhibit “E”** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

~~2.~~1. **Termination**. ~~In~~Except as otherwise provided herein, in the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA. The LEA may terminate this DPA at any time by ceasing to use the Services.

~~4.~~2. **Effect of Termination Survival**. If the Service Agreement is terminated, LEA may close LEA Educator accounts and require the Provider ~~shall~~to destroy ~~all of LEA’s~~ Student Data ~~pursuant to~~ associated with that LEA Educator account in accordance with Article IV, section 6.

~~6.~~3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including, as applicable, those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses, and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

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.

LEA Educator: Any individual educator who has signed-up for the Services using an email address issued by the LEA. LEA Educators are authorized agents of the LEA.

LEA Issued Email Address: Any email address using the following domain(s): @cvsdvt.org or any domain(s) designated by a Subscribing Provider pursuant to Exhibit "E".

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.

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 the DPA in its entirety with the Provider.

~~**Originating** LEA: An LEA who originally executes the DPA in its entirety with the Provider.~~

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

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 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 employees; (2) 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.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

~~**Service Agreement**: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.~~

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. 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" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

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.

Third Party: The term "Third Party" means a provider of digital educational software or services, including

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **CHAMPLAIN VALLEY SCHOOL DISTRICT** ("Originating LEA") which is dated ____________________, to any other LEA ("Subscribing LEA") who accepts this General Offer ~~of Privacy Terms ("General Offer") through its signature below.~~by providing a revised definition for LEA Issued Email Address below, signing below and emailing a signed copy of this Exhibit E to Flipgrid at FGExSub@microsoft.com. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. LEA Issued Email Address(es) for Subscribing LEA will be as follows: [Subscribing LEA to insert]. The Provider may unilaterally withdraw the General Offer and terminate this DPA between Provider and Subscribing LEA in the event of: (1) a material change in the applicable privacy ~~statutes~~statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:
FGExSub@microsoft.com ____.

FLIPGRID, INC.

BY: ____Date: ______________________________

Printed Name: _____________________________________Title/Position: __________________________________

2. Subscribing LEA

A Subscribing LEA, by ~~signing a separate Service Agreement with Provider~~permitting its own LEA Educators, as authorized agent of the Subscribing LEA, to agree to the Flipgrid Terms of Use and use the Services on its behalf, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the **CHAMPLAIN VALLEY SCHOOL DISTRICT** and the Provider. ~~**PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **~~

Subscribing LEA: (School District Name): ____

BY: ____Date:________________________________