

**STUDENT DATA PRIVACY AGREEMENT
VERSION (2018)**

Westwood Public Schools

and

Flipgrid, Inc.

August 14, 2020

This Student Data Privacy Agreement (“DPA”) is entered into by and between the school district, Westwood Public Schools (hereinafter referred to as “LEA” or “Local Education Agency”) and Flipgrid, Inc. (hereinafter referred to as “Provider”) on August 14, 2020 (the “Effective Date”). The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) as described in Article I and Exhibit “A”; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services may also be subject to several state laws depending on the state in which the Services are provided.

Specifically, those laws are: in Massachusetts: 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; in New Hampshire: RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and in Rhode Island: 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 this 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:

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 and, to the extent applicable under New Hampshire law, Teacher Data (as defined in Exhibit “C”) transmitted to Provider via the Services pursuant to Exhibit “A”, including compliance with all applicable Federal and state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, in Massachusetts: 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; in New Hampshire: RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and in Rhode Island: R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, R.I.G.L., 11-49.3 et. seq.; and other applicable state laws, all as may be amended from time to time. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) and Teacher Data are transmitted to Provider via the 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 the use and maintenance of Student Data and Teacher Data. Control duties are set forth below.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described in Exhibit “A” 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 in this Article and Exhibit “A”, Provider receives via the Services the categories of Student Data and Teacher Data described 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 all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data or Teacher Data transmitted to the Provider through the Services is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or Teacher Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Student Data or Teacher Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or Teacher Data contemplated per this DPA shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data and Teacher Data notwithstanding the above. The LEA may access, download and delete Student Data and Teacher Data through the LEA Educator account associated with the Grid onto which such Student Data and Teacher Data was submitted. The Provider will reasonably cooperate with any other request regarding Student Data and Teacher 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/Eligible Student Access.** Prior to using the Services, the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the Pupil’s Records, correct erroneous information, and procedures for the transfer of Pupil-Generated Content to a personal account, consistent with the functionality of Services. Provider shall cooperate and respond within ten (10) days to the LEA’s request for PII in a Pupil’s Records held by the Provider to view or correct as necessary, including any Student Data related to special education students In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records or 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. **Third Party Request.** 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 or Teacher 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 by contacting the contact provided by LEA which may be updated from time to time 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. The Provider will not use, disclose, compile, transfer, sell the Student Data or Teacher Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data, Teacher Data, and/or any portion thereof, without the express written consent of the LEA unless legally required or without a court order or lawfully issued subpoena. Student Data or Teacher Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student or teacher's use of Provider's services.
5. **No Unauthorized Use.** Provider shall not use Student Data, Teacher Data, or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions on Provider's behalf in delivery of the Services, whereby the Subprocessors agree to protect Student Data and Teacher Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws.** LEA shall provide Student Data and Teacher Data for the purposes of the DPA in compliance with any applicable provisions of the FERPA, PPRA, IDEA, and in Massachusetts: 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; in New Hampshire: RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; in Rhode Island: 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 the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected 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 State and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, in Massachusetts: 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; in New Hampshire: RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; in Rhode Island: 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 all other applicable privacy statutes and regulations.
- 2. Authorized Use.** Student Data and Teacher Data shared via the Services, including persistent unique identifiers, shall be used for no purpose other than providing the Services, as permitted under this DPA and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that except for sharing with vendors, consultants, and other third party service providers, known as Subprocessors in this DPA, who need access to Student Data to carry out work on Provider's behalf and at Provider's direction, it shall not make any re-disclosure of any Student Data, Teacher Data, or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA, or the eligible Student or parent at question unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information or such disclosure is authorized under the statutes referred to in subsection (1), above.
- 3. Employee Obligation.** Provider shall require all employees and agents who have access to Student Data or Teacher Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data or Teacher Data pursuant to the DPA.
- 4. No Disclosure.** De-identified information, as defined in Exhibit "C", may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). The Provider and LEA agree that the Provider cannot successfully de-identify information if there are fewer than twenty (20) students in the samples of a particular field or category of information collected, i.e., twenty students in a particular grade, twenty students of a particular race, or twenty students with a particular disability. Provider agrees not to attempt to re-identify de-identified Student Data and Teacher Data and not to transfer de-identified Student Data and Teacher 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. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA.

- 5. Disposition of Data.** Within sixty (60) days of the closure of an LEA Educator account, Provider shall dispose or delete all Student Data and Teacher Data obtained through the Services and retained by Provider, including but not limited to any PII hosted on a Grid associated with such LEA Educator account, where a “Grid” is a the video sharing environment managed by an LEA Educator through his or her Flipgrid account. Nothing in the DPA authorizes Provider to maintain Student Data or Teacher Data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Student Data and Teacher Data; (2) erasing or otherwise modifying the Personally Identifiable Information in those records to make it unreadable or indecipherable. Provider shall provide written notification to the email account associated with the LEA Educator on whose Grid the Data is hosted when the data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. 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 of any Student Records associated with an LEA Educator account and Students or LEA may access and export all Student Data available through my.flipgrid.com as described in Article II, Section 3 of this DPA.
- 6. Advertising Prohibition.** Provider is prohibited from leasing, renting, using or selling Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians, except that Provider may communicate about use of the Services and related support activities and events; (b) inform, influence, or enable marketing, advertising or other commercial efforts other than providing the Service to LEA 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. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.

ARTICLE V: DATA PROVISIONS

1. Data Security. The Provider is committed to helping protect the security of LEA’s information. Provider has implemented and will maintain appropriate technical and organizational measures intended to protect any Student and LEA data, including but not limited to Student and Teacher Data, against accidental, unauthorized or unlawful access, disclosure, use, modification, alteration, loss, or destruction consistent with industry standards. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.

- a. Security Training.** Flipgrid informs its personnel about relevant security procedures and their respective roles. Flipgrid also informs its personnel of possible consequences of breaching the security rules and procedures.
- b. Provider Contact.** For any questions on security, the LEA may contact support@flipgrid.com.

- c. Passwords and Employee Access.** Provider shall secure its employees' access to LEA Educator and Student usernames, passwords, and any other means of gaining access to the Services or to Student Data and Teacher Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data and Teacher Data to employees or contractors that are performing the Services. Employees with access to Student Data and Teacher Data shall have signed confidentiality agreements regarding said Student Data and Teacher Data.. All employees with access to Student Data and Teacher Data shall pass criminal background checks.
- d. Destruction of Data.** See Article IV, Section 5 above for destruction of data.
- e. Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data , including but not limited to ensuring that Teacher or Student Data is not permitted to be viewed or accessed by parties restricted from doing so under applicable law. Provider shall maintain all Teacher Data and Student Data obtained via the Services in a secure computer environment and not copy, reproduce, or transmit Teacher Data and Student Data obtained via the Services, except as necessary to provide the Services including by fulfilling data transfer requests by the LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as required in order to perform services on behalf of the Provider.
- f. Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to Student Data Further, the LEA can contact support@flipgrid.com if there are any security concerns or questions.
- g. Security Technology.** When the Services are accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data from unauthorized access. This equivalent technology shall include server authentication and data encryption. Provider shall host data collected via the Services in an environment using a firewall that is periodically updated according to industry standards.
- f. Security Coordinator.** The LEA may contact the Provider's Security Coordinator at support@flipgrid.com from the email address associated with a particular LEA Educator account to request access to the Teacher Data received by an LEA Educator account.
- g. Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data and Teacher Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.
- h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate in a timely manner any security and privacy vulnerabilities identified as critical by a Provider or third party led assessment.
- i. Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data and Teacher Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data, Teacher Data, or any portion thereof.
- j. Audits.** Upon a receipt of a request from the LEA, 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/jurisdiction in connection with any legally required audit or investigation of the LEA's use of Services.

k. Additional Data Security Requirements. 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, develop an internal system to 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.

2. Data Breach.

- a. If Provider becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Student Data or other personal information while processed by Provider (each a “Security Incident”), Provider will promptly and without undue delay (1) notify LEA of the Security Incident within ten (10) days by contacting the contact provided by the LEA Educator associated with affected Student Data or other personal information, which may be updated from time to time (where the notification is not made within 10 days it shall be accompanied by reasons for the delay); (2) investigate the Security Incident and provide LEA with detailed information via the LEA Educator as described above about the Security

- Incident, including, but not limited to, to the extent known, what happened and when, what Student Data was involved, what the LEA can do and whether notification was delayed as a result of a law enforcement investigation; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident and provide notice of those steps to the LEA via the LEA Educator as described above.
- b. 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 Security Incident.
 - c. Provider shall make reasonable efforts to assist LEA in fulfilling LEA’s obligation under applicable law or regulation to notify the relevant authorities and Students or other individuals about such Security Incident. Provider’s obligation to report or respond to a Security Incident under this section is not an acknowledgement by Provider of any fault or liability with respect to the Security Incident.
 - d. LEA must notify Provider promptly about any possible misuse of LEA Educator accounts or authentication credentials or any security incident related to the Services.
 - e. In addition, the Provider will provide the following information when it is necessary for the LEA to disclose the information under applicable law:
 - i. **The estimated number of Students and teachers affected by the Security Incident, if any.**
 - ii. **Information about any remediation services offered by the Provider to 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
 - iii. Advice on steps that the person whose information has been breached may take to protect himself or herself
 - f. Provider agrees to adhere to all applicable requirements in the Data Breach laws of the applicable state where the LEA is located and in federal law with respect to a data breach related to the Student Data and Teacher Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

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, Teacher Data, or any portion thereof and agrees to respond to inquiries emailed to support@flipgrid.com at reasonable times to answer the LEA’s questions on the written incident plan.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Term of this DPA shall be 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

Title Technology Director
Address 220 Nahatan St., Westwood, MA 02090
Telephone Number 781-326-7500 x3364
Email souellette@westwood.k12.ma.us

6. **Entire Agreement.** Except as indicated in Article VI, Section 4 above, 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.
7. **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.
8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE WHERE THE LEA IS LOCATED, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF THE COUNTY WHERE THE LEA IS LOCATED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority.** Provider represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data, Teacher Data, and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data, Teacher Data, and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data, Teacher Data, and portion thereof stored, maintained or used in any way.
10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Electronic Signature:** The parties understand and agree that they have the right to execute this DPA through paper or through electronic signature technology, which is in compliance with the applicable state law and Federal law governing electronic signatures. The parties agree that to

the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of their electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this DPA as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason in writing.

If either party would like a paper copy of this DPA, they may request a copy from the other party.

12. **Multiple Counterparts:** This DPA may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this DPA. In proving this DPA, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this DPA by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).
13. **Merger or Acquisition:** The Provider may assign to any successor through merger, sale or other disposal method its obligations and rights under this DPA. The Provider must require the successor to assume all obligations of this DPA. In the event that the Provider anticipates selling, merging or otherwise disposing of its business to a successor during the term of the DPA, the Provider shall provide written notice of the proposed sale, merger or disposal to the LEA no later than sixty (60) days prior to the anticipated date of sale, merger or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA. 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

ARTICLE VII- 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 this DPA to any other school district who signs the acceptance in said Exhibit.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Student Data Privacy Agreement as of the last day noted below.

WESTWOOD PUBLIC SCHOOLS

Steve Ouellette Date: 8/27/2020

Printed Name: Steve Ouellette Title: Director of Technology

Email address: souellette@westwood.k12.ma.us

FLIPGRID, INC.

CDM Date: 08/26/2020

Printed Name: Dr Charles Miller Title: Partner GM, Flipgrid, Microsoft

EXHIBIT “A”

DESCRIPTION OF SERVICES

Flipgrid is the leading video-discussion platform used by K12-PhD educators all over the world. Through Flipgrid’s platform on the Flipgrid.com website, the Flipgrid 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 STUDENT 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 that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred 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)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	

Category of Data	Elements	Check if used by your system
	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:	
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	

SCHEDULE OF 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 OS, Browser OS, Anonymized diagnostic data
Application Use Statistics	Meta data on user interaction with application	x
Communications	Online communications that are captured (emails, blog entries)	X – Teachers may provide feedback to students
Demographics	Date of Birth	X - when signing up for an account, Teachers are asked for their birthdate to confirm they are over 18 years of age. Once their 18+ age status is confirmed, Flipgrid does not store Teachers' birthdate information.
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	x
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
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	
	Teacher app username	X - Flipgrid provides Teachers with the option to sign up for a Flipgrid account using Google or Microsoft credentials. If Teachers choose that option, Google or Microsoft are the authentication authority and Flipgrid does store username and password information for Teachers who choose to sign up with their Google or Microsoft credentials.
	Teacher app passwords	X - Flipgrid provides Teachers with the option to sign up for a Flipgrid account using Google or Microsoft credentials. If Teachers choose that option, Google or Microsoft are the authentication authority and Flipgrid does store username and password information for Teachers who choose to sign up with their Google or Microsoft credentials.

Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	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	Teacher first name and last name.

EXHIBIT “C”

DEFINITIONS

De-Identified Information (DII): De-Identified Information or DII is former Personally Identifiable Information that has undergone De-Identification. De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information (“PII”) from Pupil Records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students and staff. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student or staff member, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. Information cannot be de-identified if there are fewer than twenty (20) students in the samples of a particular field or category, *i.e.*, twenty students in a particular grade or less than twenty students with a particular disability. For clarity, Personally Identifiable Information that has undergone De-Identification is DII and not PII.

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):

NIST 800-63-3: Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” means information that, alone or in combination, is linked or linkable to a specific student or teacher that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. PII will include, but are not limited to, Student Data, Teacher Data, and user or Pupil-Generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, teachers, or students’ parents/guardians. PII also includes, without limitation, at least the following:

First Name	Home Address
Last Name	
Telephone Number	Email Address
Discipline Records	
Special Education Data	Juvenile Dependency Records
	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	
Text Messages	
Student Identifiers	
Photos	Voice Recordings
Videos	Date of Birth
Place of birth	Social Media Address
Unique pupil identifier	Personal Biography
Credit card account number, insurance account number, and financial services account number	
Name of the student’s parents or other family members, including mother’s maiden name	

Provided that the definition of PII is met for the following elements, it may also include:

Metadata

Grades

Test results

Political Affiliations

Search Activity

Documents

Food Purchases

Grade

Classes

Subject

Religious Information

Disabilities

Socioeconomic Information

Gender, Race, Ethnicity

Attendance and mobility information between and within LEAs

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's or Staff member's Email

Information that is created and provided by a student or the student's parent to the 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

Information that is created and provided by an employee or agent of the school or LEA 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

Information that is gathered by a Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes

Teacher: Teacher means teachers, paraprofessionals, principals, school employees, contractors, and other administrators of LEAs in New Hampshire.

Teacher Data: For the purposes of this DPA, Teacher Data means PII of Teachers transmitted to Provider via the Services to the extent such PII is governed by RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100, or their successors, and Teacher Data includes, when applicable, 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.

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 Pupil Records/Teacher Records.

Pupil Generated Content: The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education 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 pupil content.

Pupil Records: Means both of the following: (1) Any PII that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

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 education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

The definition of “school official” encompasses the definition of “authorized school personnel” under 603 CMR 23.02 for Massachusetts LEAs.

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, home address, telephone number, email address, or other information allowing 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, food purchases, political affiliations, religious information, text messages, documents, 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, student identifiers, search activity, photos, voice recordings or attendance and mobility information between and within LEAs, gender, race, ethnicity geolocation information. Student Data shall constitute Pupil Records for the purposes of this DPA, and for the purposes of State and Federal 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.

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

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 software, and who has access to PII.

Third Party: The term "Third Party" means an entity that is not the Provider or LEA.






Flipgrid_Westwood

Final Audit Report

2020-08-27

Created:	2020-08-27
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA06nnFt9G4zd24NC165t9SCiqhzwd8XcK

"Flipgrid_Westwood" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2020-08-27 - 3:02:45 PM GMT- IP address: 100.1.115.187
-  Document emailed to Steven Ouellette (souellette@westwood.k12.ma.us) for signature
2020-08-27 - 3:03:32 PM GMT
-  Email viewed by Steven Ouellette (souellette@westwood.k12.ma.us)
2020-08-27 - 8:10:00 PM GMT- IP address: 66.102.6.155
-  Document e-signed by Steven Ouellette (souellette@westwood.k12.ma.us)
Signature Date: 2020-08-27 - 8:12:05 PM GMT - Time Source: server- IP address: 50.235.64.202
-  Signed document emailed to Steven Ouellette (souellette@westwood.k12.ma.us) and Ramah Hawley (rhawley@tec-coop.org)
2020-08-27 - 8:12:05 PM GMT