

VERMONT K-12 STUDENT DATA PRIVACY AGREEMENT
Version 1.0

Vermont Consortium (SDPA)
Southwest Vermont Supervisory Union
and

This Vermont Student Data Privacy Agreement ("DPA") is entered into by and between the Southwest Vermont Supervisory Union (hereinafter referred to as "LEA") and (hereinafter referred to as "Provider") on . The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated [Insert Date] ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, 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 (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; and the Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, this Agreement complies with Vermont laws and Federal Law.

WHEREAS, for the purposes of this DPA, Provider is a School Official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

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 transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, and other applicable Vermont State laws, 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. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit “A” hereto:
3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided 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 term used in the Service Agreement.

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 Agreement 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 LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** 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 respond in a timely manner (and no later than 45 days from the date of the request) to the LEA’s request for Student Data in a pupil’s records held by the Provider to view or correct as necessary. In the event that a parent of a pupil 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 pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit “A”, Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services,

the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, and all other privacy statutes.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records 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 data.
4. **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, and all other privacy statutes.
2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, 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.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.
4. **No Disclosure.** De-identified information 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). Provider agrees not to attempt to re-identify de-identified Student Data and not to

transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student 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 employ a “Request for Return or Deletion of Student Data” form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

a. Partial Disposal During Term of Service Agreement. Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA’s request to transfer data to a separate account, pursuant to Article II, section 3, above.

b. Complete Disposal Upon Termination of Service Agreement. Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit “F” hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.
 - b. **Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA’s designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
 - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
 - d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
 - e. **Security Technology.** When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.
 - f. **Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of

Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

- g. Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student 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 digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty eight (48) hours. Provider shall follow the following process:

- a.** The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
- b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - i.** The name and contact information of the reporting LEA subject to this section.
 - ii.** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii.** If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv.** Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- c.** At LEA's discretion, the security breach notification may also include any of the following:
 - i.** Information about what the agency has done to protect individuals whose information has been breached.
 - ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.

- d. Provider agrees to adhere to all requirements in applicable State and in federal law 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.
- e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
- f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI- GENERAL OFFER OF PRIVACY 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 LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. .
2. **Termination**. 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. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.
3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.
4. **Priority of Agreements**. This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes

identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

- 5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

- a. **Designated Representatives**

The designated representative for the LEA for this Agreement is:

Name: Frank Barnes
Title: Director of Educational Technology
Contact Information: fbarnes@svsu.org, 802-447-7501

The designated representative for the Provider for this Agreement is:

Name: _____
Title: _____
Contact Information: _____

- b. **Notification of Acceptance of General Offer of Terms.** Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

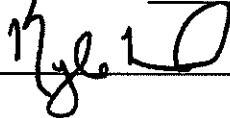
Name: _____
Title: _____
Contact Information: _____

6. **Entire Agreement.** 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 of Vermont, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction of Vermont's state and federal courts for any dispute arising out of or relating to this service agreement or the transactions contemplated hereby.
9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, 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, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.
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. **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.

[Signature Page Follows]

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

Name of Provider: FamilyID

BY:  Date: 7/23/2020

Printed Name: Kyle Ford Title/Position: CEO

Name of Local Education Agency: Southwest Vermont Supervisory Union

BY:  Date: 8/13/2020

Printed Name: Frank Barnes Title/Position: Director of Educational Technology

Note: Electronic signature not permitted.

EXHIBIT “A”

DESCRIPTION OF SERVICES

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.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
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	

Category of Data	Elements	Check if used by your system
	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	

Category of Data	Elements	Check if used by your system
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	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	

Category of Data	Elements	Check if used by your system
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. 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	

Category of Data	Elements	Check if used by your system
	Student bus card ID number	
	Other transportation data -Please specify:	
Other	Please list each additional data element used,	

Category of Data	Elements	Check if used by your system
	stored or collected by your application	

No Student Data Collected at this time _____.
 *Provider shall immediately notify LEA if this designation is no longer applicable.

**The LEA will decide what fields of information that it wants to collect from parents or students. Depending on that selection, the Provider may have none to all of the categories of data or elements above.

EXHIBIT “C”

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the 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. For purposes of this DPA, Educational Records are referred to as Student Data.

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

Operator: The term “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 primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, 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, or students’ parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, 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. Within the DPA the term "Provider" includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

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 information 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 LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement 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.

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, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Vermont 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.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

Sub-processor: For the purposes of this Agreement, the term "Sub-processor" (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.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated

content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

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 pupil records. However, for the purpose of this Agreement, 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

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

<p><u>Extent of Disposition</u></p> <p>Disposition shall be:</p>	<p>_____ Partial. The categories of data to be disposed of are as follows: [INSERT CATEGORIES]</p> <p>_____ Complete. Disposition extends to all categories of data.</p>
<p><u>Nature of Disposition</u></p> <p>Disposition shall be by:</p>	<p>_____ Destruction or deletion of data.</p> <p>_____ Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.</p>
<p><u>Timing of Disposition</u></p> <p>Data shall be disposed of by the following date:</p>	<p>_____ As soon as commercially practicable</p> <p>_____ By (Insert Date) _____</p> <p>Provider will report to LEA the actions taken to ensure the disposition of data and date on which it was completed.</p>

Authorized Representative of LEA

Date

Verification of Disposition of Data
by Authorized Representative of Provider

Date

OPTIONAL EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and the LEA to any other school district ("Subscribing LEA") who accepts this General Offer through its signature below. The Provider agrees that the information on the next page will be replaced throughout the Agreement with the information specific to the Subscribing LEA filled on the next page for the Subscribing LEA. 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 provide by LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the LEA in the event of any withdrawal so that this information may be transmitted to the Subscribing LEAs.

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA's individual information is contained below. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

SCHOOL DISTRICT NAME: _____

DATE: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name _____

Title _____

Address _____

Telephone Number _____

Email Address _____

EXHIBIT “F” DATA SECURITY REQUIREMENTS (OPTIONAL)

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]

Provider will adhere to the principles established in the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 to ensure all confidential data collected through the Provider applications is protected and secured. All controls within the Provider privacy policies follow the NIST 800-53 standards. Provider shall not use "Protected Data" (as defined above) for any other purposes than those explicitly provided for in this Agreement or provided for by agreement with the owner of the Protected Data. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Provider shall have in place sufficient internal controls to ensure that District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, if applicable.

Connections to Provider are always encrypted using TLS/SSL between users and our cloud infrastructure, and all data storage, backups, and read-replicas are encrypted using the industry standard AES-256 encryption algorithm. Data is stored in multiple databases that all reside on private networks within our cloud infrastructure, and data is never distributed, used, or accessed outside the private cloud. Provider has industry-standard policies and procedures that protect the privacy of our users, and all employees are trained on those policies. Provider also works with Premier AWS Partners to review best practices and ensure we keep current with industry standards.

- Provider employees and contractors who have access to non-public information stored by our application must submit to a background check, complete training on security practices, and agree to Provider's privacy policies. All Authorized Users are trained to maintain the confidentiality, integrity, availability, and regulatory compliance of non-public information in any format, including electronic and hard copy.
- All connections to Provider infrastructure are always encrypted between endpoints using TLS/SSL, and all sensitive information is encrypted when stored.
- All Protected Data is stored in Provider's virtual private cloud infrastructure, and data storage, backups, and read-replicas are fully encrypted using the industry standard AES-256 encryption algorithm.
- All servers that provide access to Protected Data are located in the Provider's virtual private cloud infrastructure and accessible only through load balancers on the boundaries of our private network. No public traffic is allowed on our private networks.
- All access to Provider resources is password protected using industry best-practices.
- To safeguard participants/registrants against identity theft, every registration through Provider is followed by an email confirming the transaction.

Upon termination or expiration of this agreement, Participating Educational Agencies can request Protected Data provided by and owned by the Participating Educational Agency be transitioned to a successor contractor, or deleted or destroyed. Protected Data ownership is further clarified as follows:

- Families and individuals who use the FamilyID accept the service’s Terms and Conditions as part of the service registration process. These Terms, located at <https://hello.familyid.com/terms-of-service>, describe the registrant’s rights and obligations relating to the use of the service and they constitute an agreement between the Provider and the registrant. In connection with their registration and use of the service, registrants (who may include members of participating families, parents of students, coaches and others) provide personal information about themselves and their children or other students. This information includes names, addresses, telephone numbers and the like. The registrants are responsible for all information that they provide to the service, and as listed in the Terms, they retain all ownership rights in that information. Since the Provider service enables registrants to use the service for different organizations (like other schools, camps, sports teams, etc.) they may decide to continue using the service even though they are no longer involved with the Participating Educational Agency. The registrants can maintain their information on the service, update the information or delete the information at their discretion.
- Notwithstanding anything to the contrary in this agreement, for purposes of the agreement, Student Data, Pupil Records or other similar terms defined or referenced in the agreement that include information relating to individuals or families who use the Provider’s service shall only include information that is provided by the Participating Educational Agencies. These terms shall not apply to information that is provided to the service by registrants or their related users, which will remain the sole and exclusive property of such registrants. The agreement shall not in any way require the Provider to delete any such information or take any particular actions with respect to such information. In the event of any conflict between the agreement and the foregoing terms, these terms shall apply.

All information provided by families and individuals while using the service are subject to the privacy policy located at <https://hello.familyid.com/privacy-policy> and attached below:

FamilyID, Inc. Privacy Policy

Your privacy is extremely important to us. This Privacy Policy addresses information collected by FamilyID, Inc. (“FamilyID”, “we” or “us”), and we are committed to respecting your privacy and the confidentiality of your personal data and content. To better protect you, we provide this Privacy Policy to assist you in understanding how we use and safeguard the information you provide in using our online platform (the “Platform”). In this Privacy Policy, our “Product” means the Platform and services, including those provided through our Platform; “Personal Data” means any information that we possess relating to an identified or identifiable user of the Platform, and “Program Provider” means a third party offering a program for which you are submitting information via the Platform. This Privacy Policy is incorporated into, a part of, and governed by our Terms of Service. By using the FamilyID service, you are accepting the terms

of this Privacy Policy. If you do not agree to this Privacy Policy, you may not use the FamilyID service.

1. WHAT INFORMATION DO WE COLLECT?

In order to provide you with use of the Platform, we may gather and process some or all of the following information:

- **Content:** information that is collected from or stored by you on the Platform, other than Account Sign-up Information, Customer Service Communications or Log Information.
- **Account Sign-Up Information:** information provided when you sign up for an account to use the Platform, including, your email address and password.
- **Customer Service Communications:** information that is reported to us about the operation of the Platform.
- **Log Information:** When you use the Platform, our servers automatically record basic information that your application sends in order to access our services. These server logs may include information such as your message, Internet Protocol address, other addressing information, the date and time of your request and an authentication token used to validate the identity of you and your computer.

2. HOW DO WE USE THIS INFORMATION AND FOR WHAT PURPOSE?

Our primary purpose in collecting information is to provide you with an efficient user experience. Below we describe how we use certain information. We may use this information to: provide the services and any customer support you request; resolve disputes, collect fees, and troubleshoot problems; enforce our contractual agreements; customize, measure, and improve the Platform; inform you about service updates; compare information for accuracy, and verify your identity; provide other services for you as described when we collect the information. In the future, we may give you the option of using your profile and registration data to enable FamilyID to provide you with information on relevant products, services and/or other offers.

Account Sign-up Information

We ask for Account Sign-up Information in order to verify your identity and to enable your use of the Platform.

We respect the privacy of personal e-mail accounts and we will store your e-mail addresses just as securely as other Personal Data. We will not send you unwanted e-mail messages or junk mail, and your details will not be passed to third parties for their marketing purposes without your explicit permission. However, we will use e-mail to send you messages about

Platform-related issues. We may also use e-mail to keep you up to date with news about FamilyID.

If you do not want to be kept informed in this way by e-mail, please unsubscribe at the bottom of the email message or contact us at info@familyid.com

Content

We reserve the right to pre-screen, review, flag, filter, refuse or remove any or all of Content from the Platform.

Customer Service Communications

Information which is voluntarily submitted in feedback is used for the purposes of reviewing this feedback and improving the Platform. We reserve the right to utilize anonymous information for marketing purposes, for instance by displaying selected comments on the Platform or in other communications. Further, we may from time to time ask you to provide information on your experiences which will be used to measure and improve quality. You are at no time under any obligation to provide any of such data. We will never use any personally identifiable (feedback) information without your explicit permission thereto.

Log Information

We will use this routing information to provide you with access to the Platform and for statistical information.

Children's Privacy

We are committed to protecting the privacy needs of children. Accordingly, we do not knowingly collect or solicit personal information from anyone under the age of 13 or allow such persons to register. No one under age 13 may provide any personal information to the Platform.

Student Information

Individual student data will be managed by FamilyID in accordance with the Family Educational Rights and Privacy Act of 1974 (including its implementing regulations, "FERPA") that govern the confidentiality of, and access to, students' educational records. FamilyID is committed to abide by state and federal laws protecting student data.

Requirements of Program Providers

Program Providers may have specific guidelines and limitations regarding completion and submission of registration forms and use of the information provided. FamilyID does not monitor or verify compliance with these requirements or a Program Provider's use of your information, and you are responsible for all information submitted to a Program Provider.

3. TO WHOM DO WE TRANSFER YOUR PERSONAL INFORMATION?

Except as provided below, we will not sell, rent, trade or otherwise transfer any Registration Information or Content to any third party without your explicit permission, unless we are obliged to do so under applicable laws or by order of the competent authorities.

We may share your information with our affiliates and other service providers (for example, email notification and/or payment processing services as applicable to your registration) which are providing services relating to your use of the Platform. Registration Information that you provide to us may be sent to those providers in order to deliver their services; similarly, personal information that you provide to those providers may be sent to us in order to operate the Platform. FamilyID enables you to submit your personal information to register for programs and activities, among other potential uses. When you elect to submit your personal information to a third party Program Provider or other service, organization, Provider or individual via the Platform, whether to register for a program or for any other purpose, FamilyID is not responsible for how your data is used by that third party. It is solely your responsibility to understand how and with whom that party intends to use and share your personal data. This may include the transfer of your data to other software platforms, sharing of information in the form of reports, or other methods and forms of data sharing and use.

As we continue to develop our business, we might buy or sell subsidiaries or business units. In such transactions as well as in the event all or substantially all of our assets are acquired by a third party, personal information of our users will generally be one of the transferred business assets. We reserve the right to include your personal information, collected as an asset, in any such transfer to a third party. The use of any personal information by a third party transferee shall continue to be subject to applicable law. In the event of any such transfer, notice will be posted and you may elect to discontinue your use of the Platform and/or request removal of your personal data.

We reserve the right to access, use, preserve or disclose any information we have access to if we have a good faith belief that such access, use, preservation or disclosure is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce our contractual agreements, including investigation of potential violations, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of us, our users or the public as required or permitted by law.

4. HOW DO WE PROTECT YOUR PERSONAL INFORMATION?

We take appropriate organizational and technical measures to protect the information provided to us or collected by us, and we also have protocols in place in the event we identify a security breach. Further, student data housed on the Platform is protected by us and accessible to users in a manner that is consistent with FERPA. You should be aware that internet communications are not always secure. Although we do take what we consider appropriate steps to protect your data, protection of information available over the internet is subject to attack from third parties, and accordingly we cannot guarantee that third parties cannot illegally gain access to Content.

5. HOW LONG IS YOUR PERSONAL DATA KEPT BY US?

We will retain your information for as long as is necessary to: (1) provide the use of the Platform; (2) invoice charges and to maintain records until invoices cannot be lawfully

challenged and legal proceedings may no longer be pursued; (3) communicate with you regarding other services that we offer; (4) comply with applicable legislation, regulatory requests and relevant orders from competent courts; (5) enforce our contractual agreements; or (6) fulfill any of the other purposes detailed in this Privacy Policy.

You may request removal of your information at any time. FamilyID will delete your information from the Platform within 15 days from the date of your request. Deletion of your data from the Platform will prevent you from accessing your program registration history and details regarding what data you have shared with others through the Platform. The data will be removed from back-ups at the end of the duration of the FamilyID back-up cycle, which is a minimum of 30 days and but is subject to change without notice. Please note that the Program Providers, service providers, individuals, and/or organizations that have received your information will have their own data retention practices and may be subject to regulations that require them to maintain data for a specified period of time. You must contact those entities directly regarding their use and removal of your information.

6. WHAT ARE COOKIES AND HOW DO WE USE THEM?

A cookie is a piece of data stored on the user's hard drive containing information about the user. Usage of a cookie will in no way linked to any personally identifiable information while using the Platform. Once the user closes their browser, the cookie simply terminates. For instance, by setting a cookie on our product, the user would not have to log in a password more than once, thereby saving time while on the Platform. If a user rejects the cookie, they may still use the Platform. The only drawback to this is that the user will be limited. Cookies can also enable us to track to enhance the experience using products. and for analytic purposes to help us understand the use of the Platform.

Some of our business partners may use cookies. However, we have no access to or control over these cookies.

7. HOW FAR DOES OUR RESPONSIBILITY EXTEND?

This Privacy Policy applies to services that are owned and operated by us. We do not exercise control over other users, including Program Providers to whom you submit your information, or third party systems that may use the Platform. They may place their own or other files on their systems, collect data or solicit personal information from you. We accept no responsibility or liability for these other Platforms, Program Providers, or services.

8. CAN THIS PRIVACY POLICY BE MODIFIED?

We reserve the right to modify the provisions of this Privacy Policy from time to time. By using the Platform you consent to this Policy at the time of such use. We recommend that you check this Privacy Policy periodically for any changes. FamilyID will provide notice on the platform prior to any material changes to this Policy.

9. WHAT RIGHTS DO YOU HAVE AND HOW CAN YOU CONTACT US?

If you would like to exercise your right to view, correct, complete or remove your Personal Data, please contact us at info@familyid.com. Upon verification of your identity, we will attempt to quickly fulfill your request, provided we will not act contrary to applicable legislation by fulfilling your request.