VERMONT K-12 STUDENT DATA PRIVACY AGREEMENT
Version 1.0

Mount Mansfield Unified Union School District (MMUUSD)

and

Social Sentinel, Inc.

April 17, 2020

This Vermont Student Data Privacy Agreement ("DPA") is entered into by and between the Mount Mansfield Unified Union School District (hereinafter referred to as "LEA") and Social Sentinel, Inc. (hereinafter referred to as "Provider"), on **April 17, 2020**. 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") pursuant to a contract between the parties (the "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 may be covered by one or more 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, 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 (as defined in Exhibit "C") 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 one or more of the following digital educational products and services 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, and unless unreasonably impractical given the nature and functionality of the Services.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the Student Data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions 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 Student 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, 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. Notwithstanding the foregoing, the Provider may disclose, compile, and transfer the Student Data to a Subprocessor.

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 Student 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 the LEA who has provided prior written consent for such transfer. Subsection (a) shall not apply if the de-identified Student Data provided to such party cannot reasonably be re-identified. Provider shall not copy, reproduce or transmit any Student Data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data**. Upon LEA's 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. Upon LEA's written request, 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 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 Student Data shall be subject to LEA's request to transfer Student 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 as outlined in this DPA. Prior to termination of the Service Agreement, LEA may request that Provider transfer to the extent able the Student Data to a separate account, pursuant to Article II, section 3, above.

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 or advertising 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 improve or 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**. Upon LEA's written request, 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. Notwithstanding the foregoing, to the extent that backups of the Provider's databases need to be kept intact in order to be functional in a disaster recovery (which backups may contain PII), Provider may maintain PII in its backups solely for that purpose and only as necessary for such backup and in a manner and for the duration generally accepted as a best practice for such PII.

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 Student Data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit Student Data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of 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 Student 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 ten (10) days of a verified incident. 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 applicable 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 Student Data breach.

e. Provider further acknowledges and agrees to have a written incident response plan (the "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 PII or any portion thereof, and agrees to provide LEA, upon request, with the material provisions of the Plan and shall make employees available upon reasonable notice and at reasonable times to answer questions of the LEA related to the Plan.

f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA or required by law. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall assist LEA with any legally required notification to the affected parent, legal guardian or eligible pupil of the unauthorized access, which may include the information listed in subsections (b) and (c), above

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with

LEA to 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, upon written notice from LEA, the Provider shall destroy all Student Data pursuant to Article V, Section 1.b., 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:

   The designated representative for the LEA for this Agreement is:

   Name: Jeff Wallis
   Title: Director of Technology and Network Engineering
   Contact Information: jeff.wallis@mmuusd.org 802-434-2803

   The designated representative for the Provider for this Agreement is:

   Name: Andy Vota
   Title: Director of Engineering
   Address: Social Sentinel, Inc.
   128 Lakeside Avenue
   Burlington, Vermont 05401
   Telephone Number: 802-628-0158

Email: avota@socialsentinel.com

With a copy of any notice to: Corporate Counsel, at the address above, or legal@socialsentinel.com.

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 all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, shall be bound by requirements of confidentiality and destruction of Student Data at least as strict as those contained in this DPA.

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.

SOCIAL SENTINEL, INC.

BY: Richard Gibbs (Apr 17, 2020) Date: Apr 17, 2020

Printed Name: Richard Gibbs Title/Position: President and CEO

MOUNT MANSFIELD UNIFIED UNION SCHOOL DISTRICT

BY: Jeff Wallis (Apr 17, 2020) Date: Apr 17, 2020

Printed Name: Jeff Wallis Title/Position: Director of Technology and Network Engineering

EXHIBIT "A"

DESCRIPTION OF SERVICES

- Social Media Scanning (SMS) – The SMS service reviews public social media data to identify risks and sentiment in the areas of security, public safety, harm, wellness, school climate, and acts of violence.

- Integration with G Suite (IWGS) – The IWGS service scans G Suite products associated with accounts provided by a client for potentially harmful content. The service may include the following G Suite products:
  - Integration with Gmail
  - Integration with Hangouts
  - Integration with Drive

- Integration with Microsoft (IWM) – The IWM service scans Microsoft products associated with accounts provided by a client for potentially harmful content. The service may include the following Microsoft products:
  - Integration with Outlook email

- Shareit – Shareit is a reporting platform that collects general mood indicators as well as specific incident reporting from students and other individuals.

  The Provider's platform also includes the Provider's dashboard and certain reports, analytics, trending and benchmarking data, and information provided through the services.

  Note: The Provider may change its services outlined from time to time at its sole discretion, but such changes shall not materially diminish the functionality of the services. Other than for product modifications, updates, or upgrades made in the normal course of business, the Provider will inform the LEA following material changes made to the services through release notes.

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)	X
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	

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	**Elements**	**Check if used by your system**
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	X
	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	

Category of Data	Elements	Check if used by your system
	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 -	

Category of Data	Elements	Check if used by your system
	Please specify:	
Other	Please list each additional data element used, stored or collected by your application	- Anonymous reporting tips - Public social media posts associated with school or school district

No Student Data Collected at this time _____.

* Provider shall immediately notify LEA if this designation is no longer applicable

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.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student 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, 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. Personally Identifiable Information does not include De-Identified information.

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.

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. Information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services does not constitute "Student Data" under this DPA.

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 an entity that is not the Provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

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

Extent of Disposition Disposition shall be:	____ Partial. The categories of data to be disposed of are as follows: [INSERT CATEGORIES] ____ Complete. Disposition extends to all categories of data.
Nature of Disposition Disposition shall be by:	____ Destruction or deletion of data. ____ 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.
Timing of Disposition Data shall be disposed of by the following date:	____ As soon as commercially practicable _____By (Insert Date) _____ [Insert special instructions.]

_____ _____
Authorized Representative of LEA Date

_____ _____
Verification of Disposition of Data Date
by Authorized Representative of Provider

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 though its signature below. The Provider agrees that the information below will be replaced throughout the Agreement with the information specific to the Subscribing LEA filled below 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 provided 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.

SOCIAL SENTINEL, INC.

BY: _____ Date: _____

Printed Name: Richard Gibbs Title/Position: President and CEO

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: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

COUNTY OF LEA: _____