VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

This Virginia School Data Privacy Agreement ("DPA") is entered into by and between the County School Board of York County, Virginia (hereinafter referred to as "Division") and SeeSaw. (hereinafter referred to as "Provider") on June 28 2021. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Division with certain digital educational services("Services") as described in Article I and Exhibit "A" pursuant to the Agreement entered into between the parties on June 28 2021 (Services Agreement); and

WHEREAS, in order to provide the Services described in Article 1 and Exhibit A, the Providermay receive or create and the Division may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; the Individuals withDisabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq.; and

WHEREAS, the documents and data transferred from the Division and created by the Provider's Services are also subject to several Virginia student privacy laws, including Code ofVirginia § 22.1-289.01. *School service providers; school-affiliated entities; student personal information*; and § 22.1-287.02. *Students' personally identifiable information.*

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures andduties.

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agreeto allow other Local Educational Agencies (LEAs) in Virginia the opportunity to accept and enjoy thebenefits 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 Division Data (as defined in Exhibit "C") transmitted to Provider from the Division pursuant to Exhibit "A", including compliance with all applicable state privacy statutes, including the FERPA,PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Code of Virginia § 22.1-289.01- School service

providers; school-affiliated entities; student personal information; and § 22.1-287.02-Students' personally identifiable information. In performing these Services, to the extent Personally Identifiable Information (as defined in Exhibit "C") from Pupil Records (as defined in Exhibit "C") are transmitted to Provider from Division, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the Division. Providershall be under the direct control and supervision of the Division.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digitaleducational services described below and as may be further outlined in Exhibit "A" hereto: See Exhibit A.

3. **Division Data to Be Provided**. In order to perform the Services described in this Article andExhibit "A", Provider shall list the categories of data collected, managed or shared as described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B": See Exhibit B.

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In theevent of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, the Services Agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Division Data Property of Division**. All Division Data, Student Generated Content or any other Pupil Records transmitted to the Provider pursuant to this DPA and the Services Agreement is and will continue to be the property of and under the control of the Division, or to the party who provided such data (such as the student, in the case of Student Generated Content.). The Provider further acknowledges and agrees that all copies of such Division Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Division Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Division Data or any other Pupil Records contemplated per this DPA and the Services Agreement shall remain the exclusive property of the Division. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the Divisions as it pertains to the use of Division Data notwithstanding the above. The Provider will cooperate and provide Division Data within ten (10) days at the Division's request. Provider may transfer Pupil Generated Content to a separate account, according to the procedures set forth below.

2. **Parent Access.** Provider shall cooperate and respond within ten (10) days to the Division's request for Personally Identifiable Information in Pupil 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 anyof the Pupil Records of Division Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the Division, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** Provider shall, at the request of the Division, transfer Student Generated Contentto a separate student account when required by the Code of Virginia § 22.1-289.01- School service providers; school-affiliated entities; student personal information.

4. **Third Party Request.** Provider shall notify the Division in advance of a compelled disclosure to aThird Party, unless legally prohibited.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Division Data in mannerconsistent with the terms of this DPA.

ARTICLE III: DUTIES OF DIVISION

1. **Privacy Compliance.** Division shall provide data for the purposes of the DPA and any related contract in compliance with the FERPA, PPRA, IDEA, Code of Virginia § 22.1-289.01- School service providers; school-affiliated entities; student personal information; and § 22.1-287.02- Students' Personally Identifiable Information; and, all other applicable Virginia statutes.

2. **Parent Notification of Rights** Division shall ensure that its annual notice under FERPA defines vendors, such as the Provider, as "School Officials" and what constitutes a legitimate educational interest. The Division will provide parents with a notice of the websites and online services under thisDPA for which it has consented to Student Data collection to on behalf of the parent, as permittedunder COPPA

3. **Unauthorized Access Notification.** Division shall notify Provider promptly of any known or suspected unauthorized access. Division will assist Provider in any efforts by Provider to investigateand respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all Virginia and Federal laws and regulationspertaining to data privacy and security, including FERPA, COPPA,

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

PPRA, Code of Virginia § 22.1-289.01. and § 22.1-287.02.

2. **Authorized Use**. Division Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as 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 Division Data or any portion thereof, including without limitation, anyDivision Data, metadata, user content or other non-public information and/or Personally Identifiable Information contained in the Division Data, without the express written consent of the Division, 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.

3. **Employee Obligations**. Provider shall require all employees and agents who have access to DivisionData to comply with all applicable provisions of this DPA with respect to the data shared under the Services Agreement.

4. **Use of De-Identified Information**. De-Identified Information, as defined in Exhibit "C", may be usedby 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 Information pursuant to 34 CFR 99.31(b). The Provider and Division agree that the Provider cannot successfully de-identify information if there are fewer than twenty (20) students in the samples of a particular field or category of information collected, i.e., twenty students in a particular grade, twenty students of a particular race, or twenty students with a particular disability. Provider agrees not to attempt to re-identify Division De-Identified Information and not to transfer de-identified Division 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 Division who has provided prior written consent for such transfer.

5. **Disposition of Data**. Upon written request and in accordance with the applicable terms in subsectionsbelow, Provider shall dispose or delete all Division Data obtained under the Services Agreement and this DPA when it is no longer needed for the purposes for which it was obtained. Disposition will include (1) the shredding of any hard copies of any Division 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 parties' Services Agreement or this DPA authorizes Provider to maintain Division Data obtained under the Services Agreement beyond the time reasonably needed to complete the disposition. Provider shall provide written notification when the Division Data has been disposed. The duty to dispose of Division Data shall not extend to data that has been de- identified or placed in a separate student account, pursuant to the terms of the Services Agreement and this DPA. The Division may employ a request for return or deletion of Division Data form, a copy of which is attached hereto as Exhibit D. Upon receipt of a request from the Division, the Provider will immediately provide the Division with any specified portion of the Division Data within ten (10)

calendar days of the receipt of said request.

    a. Partial Disposal During the Term of Services Agreement. Throughout the term of the Services Agreement, Division may request partial disposal of Division Data obtained under the Services Agreement that is no longer needed. Partial disposal of data shall be subject to Division's request to transfer data to a separate account, pursuant to Article II Section 3, above.

    b. Complete Disposal upon Termination of Services Agreement. Upon termination of the Services Agreement Provider shall dispose or Securely Destroy all Division Data obtained under the Services Agreement. Prior to disposal of the data, Provider shall notify Division in writing of its option to transfer data to a separate account, pursuant to Article 2, 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 Division that data will not be transferred to a separate account.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Division 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 Services to Division; or (d) use the Division Data for the development of commercial products or services, other than as necessary to provide the Service to Division. This section does not prohibit Provider from generating legitimate personalized learning recommendations or other activities permitted under Code of Virginia § 22.1-289.01.

7. **Penalties.** The failure to comply with the requirements of this DPA could subject Provider and any Third Party to all allowable penalties assessable against Provider under state and federal law. In the event the Family Policy Compliance Office of the U.S. Department of Education determines that Provider improperly disclosed Personally Identifiable Information obtained from the Division's education records, the Division may not allow Provider access to the Division's education records for at least five years.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information and makes use of appropriate administrative, technological, and physical safeguards. The general security duties of Provider are set forth below. These duties shall include, but are

not limited to:

a. **Passwords and Employee Access**. Provider shall secure and manage usernames,passwords, and any other means of gaining access to the Services or to Division Data, at levels suggested by NIST SP800-171 (Password complexity, encryption,and re-use) , NIST SP800-53 (IA control Family), and NIST 800-63-3 (Digital Identity), and NIST SP800-63B (Authenticator and Verifier Requirements) or equivalent industry best practices.

b. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the collection, storage or transmission of any data, includingensuring 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 DPA in a secure computer environment.

c. **Provider Employee Training**. The Provider shall provide annual security training tothose of its employees who operate or have access to the system.

d. **Security Technology**. When the service is accessed using a supported web browser,FIPS 140-2 validated transmission encryption protocols, or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall follow National Institute of Standards and Technology (NIST) 800- 171, or equivalent industry best practices.

e. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon Division's written request, Provider shall make the results of findings available to the Division. The Division shall treat such audit reports as Provider's Confidential Information under this DPA.

f. **Backups and Audit Trails, Data Authenticity and Integrity**. Provider will take reasonable measures, including all backups and audit trails, to protect Division Data, as defined in Exhibit C, against deterioration or degradation of data quality and authenticity. Provider shall be responsible for ensuring that Division Data is retrievable in a reasonable format.

g. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Division 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 thisArticle.

2. **Unauthorized Access or Data Breach**. In the event that Division Data is reasonably believed by the Provider or Division to have been disclosed (lost, accessed or obtained) in violation of the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) or other federal or state law applicable to such information, accessed or obtained by an unauthorized individual, Provider shall follow the following process:

   a. provide immediate notification to Division upon verification of the incident and allowthe Division or its authorized representatives to fully participate in the investigation ofthe incident.

   b. notification will be provided to the contact(s) identified in ARTICLE VII, M: Notice, and sent via email and postal mail. Such notification shall include the

      i. date, estimated date, or date range of the loss or disclosure;

      i. Division Data that was or is reasonably believed to have been lost ordisclosed;

      ii. remedial measures taken or planned in response to the loss or disclosure and to prevent further access.

   c. immediately take action to prevent further access;

   d. take all legally required, reasonable, and customary measures in working with Division to remediate the breach, which may include toll free telephone support withinformed customer services staff to address questions by affected parties and/or provide monitoring services if necessary given the nature and scope of the loss or disclosure;

   e. cooperate with Division efforts to communicate to affected parties.

   f. Provider is prohibited from directly contacting parents, legal guardians or eligible students unless expressly requested by Division. If Division 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 subsection (b) above. If requested by Division, Provider shall reimburse Division for costs incurred to notify parents/families of a breach not originating fromDivision's use of the Service.

g. the Provider shall indemnify and hold harmless the Division from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or inconnection with the breach by the Provider or any of its officers, directors, employees, agents or representatives of the obligations of the Provider's or its authorized representatives under this provision or under a Confidentiality Agreement, as the case may be.

ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS

The Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offerattached hereto as Exhibit "E"), be bound by the terms of this DPA to any other Division who signsthe acceptance in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

A. **Term**. The Provider shall be bound by this DPA for so long as the Provider maintains or possesses any Division Data.

B. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as the Services Agreement or terms of service, to the extent one exists, has lapsed or has been terminated. The Division may terminate this DPA and the Services Agreement or contract in the event of a material breach of the terms of this DPA.

C. **Data Transfer Upon Termination or Expiration**. Provider will notify the Division of impending cessation of its business and any contingency plans. Provider shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the Division. As mutually agreed upon and as applicable, Provider will work closelywith its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the Division, all such work to be coordinated and performed in advance of the formal, transition date.

D. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall destroy all of Division's Data pursuant to Article IV, section 5(b). The Provider's obligations under this DPA shall survive termination of this DPA until all Division Data has been returned or Securely Destroyed, as defined in Exhibit C.

E. **Priority of Agreements**. This DPA supersedes all end user and "click-thru" agreements. In the eventthere is conflict between the terms of the DPA and any other writing, such as the Services Agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and

take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.

F. **Amendments**: This DPA may be amended and the observance of any provision of this DPA may bewaived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties

G. **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 theparties, 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.

H. **Governing Law: Venue and Jurisdiction**. This DPA will be governed by and construed in accordance with the laws of the Commonwealth of Virginia, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction to the state and federal courts of the County of York, Virginia, or the division specified in Exhibit E as applicable, for any dispute arising out of or relating to this DPA or the transactions contemplated hereby.

I. **Authority**. Provider represents that it is authorized to bind to the terms of this DPA, including
confidentiality and destruction of Division Data and any portion thereof contained therein, all relatedor associated institutions, individuals, employees or contractors who may have access to the DivisionData and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Division Data and portion thereof stored, maintained or used in any way.

J. **Waiver**. No delay or omission of the Division to exercise any right hereunder shall be construed as a waiver of any such right and the Division reserves the right to exercise any such right from time to time,as often as may be deemed expedient.

K. **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 ofall or substantially all of the assets of such business.

L. **Electronic Signature:** The parties understand and agree that they have the right to

execute this DPA through paper or through electronic signature technology, which is in compliance withVirginia and Federal law governing electronic signatures. The parties agree that to the extent theysign electronically, their electronic signature is the legally binding equivalent to their handwrittensignature. Whenever they execute an electronic signature, it has the same validity and meaning astheir handwritten signature.

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

a. Designated Representative

The designated representative for the Provider for this DPA is:

Name: <u>Megan Bradley</u>

Title: <u>Data Protection Officer</u>

Address: <u>180 Montgomery Street, Suite 750, San Francisco, CA 94104</u>

Email: <u>megan@seesaw.me</u>

Phone: <u>415-870-4468</u>

The designated representative for the Division for this DPA is:

Name: <u>Margaret Harris-Shoates</u>

Title: <u>Coordinator of Education</u>

Address: <u>302 Dare Rd, Yorktown, VA 23692</u>

Email: <u>Mharris-shoates@ycsd.york.va.us</u>

Phone: <u>757-833-2148</u>

b. Notification of Acceptance of General Offer of Terms.
Upon execution of Exhibit E General Offer of Terms, Subscribing Division, as defined in Exhibit C, shall provide notice of such acceptance in writing and given by personal delivery or email 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 named title contact information.

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

Name: <u>Megan Bradley</u>

Title: <u>Data Protection Officer</u>

Address: <u>180 Montgomery Street, Suite 750, San Francisco, CA 94104</u>

Email: <u>megan@seesaw.me</u>

Phone: <u>415-870-4468</u>

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Virginia

Student Data Privacy Agreement as of the last day noted below.

Provider Signature _____

Date: 7/6/2021

Printed Name: Megan Bradley

Title: Data Protection Officer

Division Signature _____

Date: _____ 7-7-21

Printed Name: Victor D. Shandor, Ed.D.

Title: Superintendent

EXHIBIT "A"

DESCRIPTION OF SERVICES

Seesaw inspires engagement by giving students powerful creative tools to capture their learning. Students are even more motivated knowing they can show their learning to classmates, teachers, and families right in the app. Seesaw for Schools has additional features for districts that want to roll out Seesaw district-wide.

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

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	☐
	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	☒

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

Parent/ Guardian ID	Parent ID number (created to link parents to students)	☒
Parent/ Guardian Name	First and/or Last	☒
Schedule	Student scheduled courses	☐
	Teacher names	☒
Special Indicator	English language learner information	☐
	Low income status	☐
	Medical alerts /health data	☐
	Student disability information	☐
	Specialized education services (IEP or 504)	☐
	Living situations (homeless/ foster care)	☐
	Other indicator information- Please specify:	☐
Student Contact Information	Address	☐
	Email	☒
	Phone	☐
Student Identifiers	Local (School district) ID	☒

	number	☐
	State ID number	☐
	Provider/App assigned student ID number	☒
	Student app username	☒
	Student app passwords	☒
Student Name	First and/or Last	☒
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:	☐		Other transportation data –Please specify:	☐
Transcript	Student course grades	☐	Other	Please list each additional data element used, stored or collected by your application	☐
	Student course data	☐			
	Student course grades/perfor-mance scores	☐			
	Other transcript data –Please specify:	☐			
Transportation	Student bus assignment	☐			
	Student pick up and/or drop off location	☐			
	Student bus card ID number	☐			

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

OTHER: Use this box, if more space needed.

EXHIBIT "C"

DEFINITIONS

Data Breach means an event in which Division Data is exposed to unauthorized disclosure,access, alteration or use.

Division Data includes all business, employment, operational and Personally Identifiable Information that Division provides to Provider and that is not intentionally made generally available by the Division on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and student, employees, andpersonnel data, Student Generated Content and metadata but specifically excludes Provider data (as defined in the Services Agreement).

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from studentrecords in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. Anonymization or de-identification should follow guidance equivalent to that provided by U.S Department of Education publication "Data De-identification: An Overview of Basic Terms" or NISTIR Special Publication (SP) 8053 De-Identification of Personally Identifiable Information. The Provider's specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. Information cannot be de- identified if there are fewer than twenty (20) students in the samples of a particular field orcategory, i.e., twenty students in a particular grade or less than twenty students with a particular disability.

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

Personally Identifiable Information (PII): The terms "Personally Identifiable Information"or "PII" shall include, but are not limited to, Student Data, staff data, parent 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 byDivision or its users, students, or students' parents/guardians, including "directory information" as

defined by §22.1-287.1 of the Code of Virginia".

PII includes, without limitation, at least the following:

- Staff, Student or Parent First, Middle and Last Name
- Staff, Student or Parent Telephone Number(s)
- User Name/User ID
- Discipline Records
- Special Education Data
- Grades
- Criminal Records
- Health Records
- Biometric Information
- Socioeconomic Information
- Political Affiliations
- Text or Instant Messages
- Student Identifiers Photos
- Videos
- Grade
- Home Address Subject
- Email Address
- Test Results
- Juvenile Dependency Records Evaluations
- Medical Records
- Social Security Number
- Disabilities
- Food Purchases
- Religious Information Documents
- Search Activity
- Voice Recordings
- Date of Birth
- Classes
- Information in the Student's Educational Record
- Information in the Student's Email

Provider: For purposes of the DPA, the term "Provider" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Pupil Records.

Pupil Generated Content: The term "Pupil Generated Content" means materials or content created by a student 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 student content.

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

Securely Destroy: Securely Destroy means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards of Technology (NIST) SP 800-88 Appendix A guidelines relevant to sanitization of data categorized as high security. All attempts to overwrite magnetic data for this purpose must utilize DOD approved methodologies.

School Official: For the purposes of this DPA and pursuant to 34 CFR 99.31 (B), aSchool 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 ofPersonally Identifiable Information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by Division 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 andlast 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 DPA, and for the purposes of Virginia 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. Anonymization or de-identification should guidance equivalent to that provided by U.S Department of Education publication "Data De-identification: An Overview of Basic Terms" or NISTIR Special Publication (SP) 8053 De-Identification of Personally Identifiable Information.

Student Generated Content: Alternatively known as user-created content (UCC), is any form of content, such as images, videos, text and audio, that have been created and posted by student users on online platforms.

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

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than Division or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

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

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

The County School Board of York County, Virginia, (Division), directs SeeSaw (Provider), to dispose of data obtained by Provider pursuant to the terms of the DPA between Division and Provider. The terms of the Disposition are setforth below:

1. Extent of Disposition

[ ] Disposition is Complete. Disposition extends to all categories of data.

[ ] Disposition is partial. The categories of data to be disposed of are set forth below or are found inan attachment to this Directive:

     [Insert categories of data]

2. Nature of Disposition

[ ] Disposition shall be by destruction or secure deletion of data.

[ ] Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

     [Insert or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date:
[ ] As soon as commercially practicable
[ ] By (Insert Date]

4. Signature of Authorized Representative of Division

BY:_____   Date: _____

Printed Name:_____   Title/Position:_____

5. Verification of Disposition of Data

BY:_____   Date: _____

Printed Name:_____   Title/Position:_____

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

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 Division to any other school division ("Subscribing Division") who accepts this General Offer though its signature below. The Provider agrees that the information on the next page will be replaced throughout the DPA with the information specific to the Subscribing Division filled on the next page for the Subscribing Division. 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 Division may also agree to change the data provided by Division to the Provider to suit the unique needs of the Subscribing Division. The Provider may withdraw the General Offer in the event of: (1)a material change in the applicable privacy statues; (2) a material change in the services and productssubject listed in the originating Services Agreement; or (3) after three years from the date of Provider's signature to this form. Provider shall notify the Division in the event of any withdrawal sothat this information may be transmitted to the Subscribing Divisions.

By: _____   Date: 7/6/21 _____

Printed Name: Megan Bradley _____   Title/Position: Data Protection Officer

2. Subscribing Division

A Subscribing Division, by signing a separate Services Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing Division's individual information is contained on the next page. The Subscribing Division and the Provider shall thereforebe bound by the same terms of this DPA.

BY: _____   Date: _____

Printed Name: _____   Title/Position _____

TO ACCEPT THE GENERAL OFFER THE SUBSCRIBING DIVISION MUST DELIVERTHIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW

BY: _____   Date: 7/6/21 _____

Printed Name: Megan Bradley _____   Title/Position: Data Protection Officer

Email Address privacy@seesaw.me _____