

## **VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

Agency Code: 6655

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 NWEA (hereinafter referred to as “Provider”) on \_\_\_\_\_ 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 Custom Master Subscription Agreement entered into between the parties on August 1, 2021 (Services Agreement); and

**WHEREAS**, in order to provide the Services described in Article 1 and Exhibit A, the Provider may receive or create and the Division may provide documents or data that as applicable to Provider may be 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, Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 *et. seq.*; and

**WHEREAS**, the documents and data transferred from the Division and created by the Provider’s Services may also be subject to applicable Virginia student privacy laws, including 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*.

**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 the Services Agreement to establish implementing procedures and duties.

**WHEREAS**, the Provider may, by signing the “General Offer of Privacy Terms” (Exhibit “E”), agree to allow other Local Educational Agencies (LEAs) in Virginia 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 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, which may include 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. Providers shall be under the direct control and supervision of the Division.

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

## VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

See Exhibit A

3. **Division Data to Be Provided.** In order to perform the Services described in this Article and Exhibit "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 the event of a conflict, definitions used in the Services Agreement shall prevail over terms in this DPA.

### **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, provided they contain PII, are also subject to the provisions of this DPA and the Services Agreement 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. Division may access its Division Data via self-service from Provider's administrative and reporting system during its license and within 30 days of expiration or termination of its license. 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) business days to the Division's request for Personally Identifiable Information in Pupil Records held by the Provider to correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of 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.** Division may transfer Student Generated Content to a separate student account when required by the Code of Virginia § 22.1-289.01- School service providers; school-affiliated entities; student personal information by accessing its Division Data from Provider's administrative and reporting system.
4. **Third Party Request.** Provider shall notify the Division in advance of a compelled disclosure to a Third Party, unless legally prohibited.

## **VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

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 a manner materially consistent 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 the Services Agreement and any related contract in compliance, as applicable, 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 this DPA for which it has consented to Student Data collection to on behalf of the parent, as permitted under COPPA
3. **Unauthorized Access Notification.** Division shall notify Provider without undue delay of a Data Breach. Division will assist Provider in any efforts by Provider to investigate and respond to any Data Breach.

### **ARTICLE IV: DUTIES OF PROVIDER**

1. **Privacy Compliance.** The Provider shall comply with all applicable Virginia and Federal laws and regulations pertaining to data privacy and security, which may include FERPA, 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 the Services Agreement and as authorized under the applicable statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any 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 Division Data 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 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 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 ten (10) 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

## **VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

de-identified Division Data to any party unless that party agrees in writing not to attempt re-identification.

5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsections below, 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 De- Identified Information or Division Data 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 make available to the Division a complete and secure download of the data file in Provider's administration and reporting system within thirty (30) calendar days of the receipt of said request.
  - a. **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 use industry standard practices 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 reasonably secure and manage usernames, passwords, and any other means of gaining access to the Services or

## **VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

to Division Data, at industry standard levels.

- b. Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the collection, storage or transmission of any data, including, ~~and~~ that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Division Data under the DPA or the Services Agreement in a secure computer environment.
- c. Provider Employee Training.** The Provider shall provide annual security training to those 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 across public network to protect data from unauthorized access. The service security measures shall follow National Institute of Standards and Technology (NIST) 800- 57, or equivalent industry standards.
- e. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any material identified security and privacy vulnerabilities in a timely manner.
- f. Backups** Provider will take reasonable measures to maintain backups, at least daily, of Student Data in case of Provider's system failure or other unforeseen event resulting in loss of Student Data or any portion thereof.
- g. Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Division Data in a manner materially 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.

**Unauthorized Access or Data Breach.** In the event of a Data Breach, Provider shall follow the following process:

- a.** provide notification to Division within seventy-two (72) hours upon verification of the Data Breach and reasonably coordinate with the Division or its authorized representatives in the investigation of the Security Breach..
- b.** notification will be provided to the contact(s) identified in ARTICLE VII, M: Notice, and sent via email. Such notification shall include to the extent known at such time, the
  - i.** date, estimated date, or date range of the Data Breach ; and
  - i.** Division Data that was or is reasonably believed to have been the subject of the Data Breach ;
  - ii.** remedial measures taken or planned in response to the Data Breach to prevent further access.
- c.** immediately take action to prevent further unauthorized access;
- d.** take all applicable and legally required, reasonable, and customary measures in

## **VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

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. reasonably 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 a Data Breach, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the Data Breach, which shall include the information listed in subsection (b) above provided the Division gives Provider the contact information for such parent, legal guardian or eligible pupil. If requested by Division, Provider shall reimburse Division for the actual, reasonable costs incurred to provide any applicable and legally required notification to individuals affected by a Security Breach not originating from Division's use of the Service.

## **ARTICLE VII: MISCELLANEOUS**

- A. **Term**. The term of this DPA shall be for a period of one (1) year
- B. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent, or upon a material breach of this DPA and the breaching party fails to cure such breach within thirty (30) days of written notice from the non-breaching party .
- C. **Data Transfer Upon Termination or Expiration**. Provider will notify the Division of any impending cessation of its business and any contingency plans.
- D. **Effect of Termination Survival**. If the DPA is terminated or has expired, the Provider shall upon Division request within sixty (60) days of such termination or expiration, return to the Division or securely dispose of all Division Data in its possession or in the possession of Authorized Persons and notify the Division that such Division Data has been returned to the Division or disposed of securely. If Provider is not reasonably able to return or securely dispose of Division Data, including, but not limited to, Division Data stored on backup media, the Provider will continue to protect such Division Data in accordance with the terms of this DPA until such time that it can reasonably return or securely dispose of such Division Data.
- E. **Priority of Agreements**. In the event there 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 be waived (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,

**VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

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.

- 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 for any dispute arising out of or relating to this DPA or the transactions contemplated hereby.
- I. **Authority.** Provider will have appropriate agreements in place with confidentiality terms and other obligations sufficient to protect Personal Information in accordance with this DPA with its associated institutions, individuals, employees or contractors who have a need to know or may otherwise have access to the DivisionData and/or any portion thereof,.
- J. **Waiver.** No delay or omission of either party to exercise any right hereunder shall be construed as a waiver of any such right and the parties reserve 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 of all 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 with Virginia and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature.
- 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 designated representatives before:

**a. Designated Representatives**

The designated representative for the Provider for this DPA is:

Name:	Jacob Carroll
Title:	Sr. Director, Privacy & Information Security
Address:	121 NW Everett St., Portland, OR 97209
eMail:	legalservices@nwea.org
Virginia School Data Privacy	503-548-5281

## **VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

Phone:

The designated representative for the Division for this DPA is:

Name:	Leeza Beazlie
Title:	Coordinator of Testing and Accountability
Address:	302 Dare Rd Yorktown, VA 23692
eMail:	<a href="mailto:lbeazlie@ycsd.york.va.us">lbeazlie@ycsd.york.va.us</a>
Phone:	757-898-0463



**VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

*[Signature Page Follows]*

**VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

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

DocuSigned by:  
*Geri Cohen*  
9EE11D7374704BD...

Provider Signature

Date: 8/26/2021

Printed Name: Geri Cohen

Title: CFO & EVP, Corporate Services

Division Signature *Victor D Shander*

Date: 8/23/21

Printed Name: Victor D Shander

Title: Superintendent

**VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

**EXHIBIT "A"**

**DESCRIPTION OF SERVICES**

**[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE]**

**Products: MAP® Growth**

**NWEA® is a research-based, not-for-profit organization that supports students and educators worldwide by creating assessment solutions that precisely measure growth, proficiency or fluency and provide insights to help tailor instruction. See the Services Agreement for additional details.**

## 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.	<input type="checkbox"/>
	Other application technology meta data- Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data- Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications that are captured (emails, blog entries)	<input type="checkbox"/>

Conduct	Conduct or behavioral data	
Demographics	Date of Birth	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, preferred or primary language spoken by student)	<input type="checkbox"/>
	Other demographic information- Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information- Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>

## VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

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

	number	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm. reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>
Student work	Student generated content; writing, pictures etc.	<input type="checkbox"/>
	Other student	<input type="checkbox"/>

## VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

	work data - Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/perfor- mance scores	<input type="checkbox"/>
	Other transcript data -Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>

	Other transportation data -Please specify:	<input type="checkbox"/>
Other	Please list each additional data element used, stored or collected by your application	<input type="checkbox"/>

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.

# **VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

## **EXHIBIT "C"**

### **DEFINITIONS**

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

**Division Data** includes all student Personally Identifiable Information that Division provides to Provider and that is not intentionally made generally available by the Division on public websites or publications but specifically excludes Provider data (as defined in the Services Agreement).

**De-Identifiable Information (DI):** De-Identification refers to the process by which the Provider 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. 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 or category, 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 a reasonable 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 personally identifiable Student Data, staff data, parent data, metadata, and user or Pupil Generated Content provided to Provider's software, website, service, or app, including mobile apps., PII may include, to the extent identifiable, without limitation, 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

## **VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

- 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 PII that directly relates to a student that is maintained by Division and (2) any PII 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), 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



## **VIRGINIA SCHOOL DATA PRIVACY AGREEMENT**

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 PII 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 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 that contain PII for the purposes of this DPA. Student Data as specified in Exhibit Bis 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 has PII and 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 NWEA, (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 set forth 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 in an 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:

[Upon request, 60 days from termination.]

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: \_\_\_\_\_