

MAINE STUDENT DATA PRIVACY AGREEMENT
Version 1.0

Maine School Administrative District #6

and

NWEA

September 1, 2020

This Maine Student Data Privacy Agreement ("DPA") is entered into by and between the **Maine School Administrative District #6** (hereinafter referred to as "School Unit") and NWEA (hereinafter referred to as "Provider") on the date provided on the preceding page. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the School Unit with certain digital educational services via Provider's Assessment System ("Services") pursuant to a Master Subscription Agreement ("MSA") between the parties effective September 1, 2020 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the School Unit may provide, documents or Student Data that are covered by several federal statutes, among them as applicable, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. §1232g et. seq. (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. §1232h et. seq.; and Individuals with Disabilities Education Act ("IDEA") 20 U.S.C. § 1400 et. seq. (34 CFR Part 300); and

WHEREAS, the documents and Student Data transferred from School Units and created by the Provider's Services are also subject to several state student privacy laws, including Maine's dissemination of student records law 20-A M.R.S. §6001; Maine Student Information Privacy Act 20-A M.R.S. §951 et. seq. ("MSIPA"); and Maine Unified Special Education Regulations ("MUSER") Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, this Agreement complies with Maine laws, and federal law as applicable; 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" attached hereto as Schedule "E", agree to allow other school units in Maine the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

- 1. Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the School Unit pursuant to the Service Agreement, including compliance with all applicable federal and state privacy statutes, including FERPA, PPRA, COPPA, IDEA, MSIPA, and MUSER and other applicable Maine 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 School Unit. Provider shall be under the direct control and supervision

of the School Unit with respect to the use and maintenance of information shared with Provider by School Unit pursuant to this Agreement and the Service Agreement.

- 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:

MAP Growth, MAP Skills, and MAP Reading Fluency (collectively the “Assessment System”), see complete description in Exhibit A

- 3. Student Data to Be Provided.** In order to perform the Services described in the Service Agreement, School Unit shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit “B”:

Student demographic information, grade level, courses, teachers

- **See Exhibit “B” for additional data that may be provided.**

- 4. DPA Definitions.** The definition of terms used in this DPA is found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

- 1. Student Data Property of School Unit.** 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 School Unit. 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 DPA 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 shall remain the exclusive property of the School Unit. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the School Unit as it pertains to the use of Student Data notwithstanding the above.
- 2. Parent Access.** School Unit shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data on the pupil’s records and correct erroneous information, consistent with the functionality of services. Provider shall make the Student Data accessible for download by the School Unit within the Assessment System in .CSV format no later than 30 days. 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 School Unit, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** Reserved.
4. **Third Party Request.** Should a Third Party, including law enforcement, former employees of the School Unit, current employees of the School Unit, and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the School Unit. Provider shall notify the School Unit in advance of a compelled disclosure to a Third Party. The Provider will not use, disclose, compile, transfer, and/or sell the Student Data and/or any PII portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any PII portion thereof.
5. **No Unauthorized Use.** Provider shall not use Student Data for any purpose other than as explicitly specified in the Service Agreement. Any use of Student Data shall comply with the terms of this DPA.
6. **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 a manner materially consistent with the terms of this DPA.

ARTICLE III: DUTIES OF SCHOOL UNIT

1. **Provide Data In Compliance With FERPA.** School Unit shall provide data for the purposes of the Service Agreement in compliance with the applicable provisions of FERPA, COPPA, PPRA, IDEA, MSIPA, and MUSER and all other Maine privacy statutes and regulations referenced or identified in this DPA.
2. **Annual Notification of Rights.** If the School Unit has a policy of disclosing education records under 34 CFR § 99.31 (a) (1), School Unit 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, and determine whether Provider qualifies as a “school official.”
3. **Reasonable Precautions.** School Unit 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.** School Unit shall notify Provider promptly of any known or suspected unauthorized access. School Unit 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, PPRRA, IDEA, MSIPA, MUSER and all other Maine privacy statutes and regulations identified in this DPA.

Authorized Use. The data shared pursuant to the Service Agreement, including persistent unique identifiers (to the extent such identifiers are PII), shall be used for no purpose other than the Services stated in the Service Agreement and 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 PII portion thereof, including without limitation, meta data, user content or other non-public information that is PII and personally identifiable information contained in the Student Data, without the express written consent of the School Unit.

2. **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. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
3. **No Disclosure.** Anonymized and De-identified Data 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) and as set forth in the Service Agreement, provided such use complies with FERPA and other applicable state and federal law. 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 School Unit, who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill this Agreement or the Service Agreement, provided such copying, reproduction, or transmission is permitted by this Agreement.
4. **Disposition of Data.** Provider shall dispose of, delete, or De-identify, materially in accordance with NIST Special Publication 800-88 and FERPA and other applicable state and federal laws, all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said Student Data to School Unit or School Unit's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. 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. Disposition shall include: (1) shredding any and all hard copies of any Student Data; and (2) erasing or otherwise modifying the records to make them unreadable and indecipherable. Provider shall provide written notification to School Unit when the Student Data has been disposed of or deleted. The duty to dispose of or delete Student Data shall not extend to data that has been Anonymized or De-identified, pursuant to the other terms of the DPA. The School Unit may employ a "Directive for Disposition of Data" Form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the School Unit, the Provider will immediately provide the School Unit with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

5. **Advertising Prohibition.** Without limiting any other provision in this DPA, Provider is specifically prohibited from using, disclosing, or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service(s) to School Unit; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service(s) to School Unit.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain commercially reasonable data security measures, consistent with industry standards, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person in accordance with the Security section of Provider's Privacy Policy – Assessment System located at <https://legal.nwea.org/nwea-privacy-and-security-for-pii.html>. 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 reasonably secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at an industry standard level. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees and contractors with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks. Notwithstanding the foregoing, School Unit is solely responsible for configuring role-based access to Student Data within the Assessment System and for ensuring the security and availability of School Unit's own passwords, computers, computer networks, and internet connections, including security patches, choice of browser and browser configuration settings to be used with the Services, email, and other transmissions. School Unit acknowledges that its systems administrator controls the access and security points of the Services.
 - b. **Destruction of Data.** Provider shall destroy, delete, or De-identify all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and , prior to doing so, shall make available to the School Unit a complete and secure download of the data file in .CSV format. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
 - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by School Unit.
 - 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 School Unit with contact information of an employee who School Unit may contact if there are any security concerns or questions.

- e. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer (“SSL”) or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.
 - f. **Security Coordinator.** 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 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.
 - h. **Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified material security and privacy vulnerabilities in a timely manner. Upon request from School Unit, Provider shall provide School Unit with records evidencing completion of such periodic risk assessments and documenting any identified material security and privacy vulnerabilities as well as the remedial measures taken to correct them.
 - i. **Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider’s system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.
 - j. **Audits.** Upon request not more than once annually, School Unit may request Provider’s SOC Type 2 audit report, provided School Unit treats such report as confidential information and does not disclose it to a third party.
2. **Data Breach.** In the event that Student Data has been confirmed to have been accessed or obtained by an unauthorized individual, Provider shall provide notification to School Unit within a reasonable amount of time of the incident. Provider shall follow the following process for such notification:
- a. The security breach notification shall be written in plain language, titled similarly to “Notice of Data Breach” and including detailed information regarding what happened, what information was involved, what Provider is doing, and what the School Unit can do. 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 School Unit subject to this section.
 - ii.** A list of the types of Student Data that were or are reasonably believed to have been the subject of a confirmed 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 School Unit’s discretion, and upon School Unit’s request, a supplement to the security breach notification will be provided that shall 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 themselves.
- d.** Provider agrees to adhere to all requirements in applicable state and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such confirmed data breach.
- e.** Provider further acknowledges and agrees to have a written incident response plan that reflects industry standard practices and is consistent with industry standards and federal and state law for responding to a confirmed data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including Student Data and agrees to provide School Unit, upon request, with a copy of said written incident response plan.
- f.** At the request and with the assistance of School Unit, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above, provided LEA gives NWEA the contact information for the parent, legal guardian or eligible student.

ARTICLE VI- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit “E”), be bound by the terms of this to any other School Unit 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. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than one (1) year.
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.
3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall dispose of and destroy all Student Data in accordance with the DPA and Service Agreement.
4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, terms of use, or privacy policy, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph, 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, 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:

The designated representative for the Provider for this Agreement is:

Jacob Carroll: Sr. Director, Privacy & Information Security

Address: Address: 121 NW Everett St, Portland, OR 97209

Email: jacob.carroll@nwea.org

Phone: 503-548-5281

The designated representative for the School Unit for this Agreement is:

Scott Nason, Director of Technology
290B Parker Farm Road, Buxton, ME 04093
snason@bonnyeagle.org
207-929-2325

6. **Entire Agreement**. This DPA and the Services Agreement 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. To the extent this


DPA and the Service Agreement conflict, this DPA will control. 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 MAINE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS IN CUMBERLAND COUNTY, MAINE FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority**. Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.
10. **Waiver**. No delay or omission of either party to exercise any right hereunder shall be construed as a waiver of any such right and each party reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

[Signature Page Follows]

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

NWEA

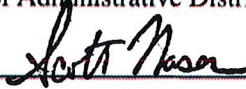
BY:  Date: 1/12/2021

Printed Name: Gerri Cohen Title/Position: CFO & EVP, Corporate Services

Address for Notice Purposes:

121 NW Everett Street
Portland, OR 97209

Maine School Administrative District #6

BY:  Date: 1/13/2021

Printed Name: Scott Nason Title/Position: Director of Technology

Address for Notice Purposes:

290B Parker Farm Road
Buxton, ME 04093

EXHIBIT “A”

DESCRIPTION OF SERVICES

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 MSA for additional details.

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	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X

Category of Data	Elements	Check if used by your system
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	x
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	

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

Category of Data	Elements	Check if used by your system
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

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

Category of Data	Elements	Check if used by your system
Other	Please list each additional data element used, stored or collected by your application:	

EXHIBIT “C”

DEFINITIONS

METDA (Maine Educational Technology Directors Association): Refers to the membership organization serving educational IT professionals in the state of Maine to promote general recognition of the role of IT professionals in educational institutions; improve network and computer services; integrate emerging technologies; encourage appropriate use of information technology for the improvement of education and support standards whereby common interchanges of electronic information can be accomplished efficiently and effectively.

Covered Information: Covered Information means materials that regard a student that are in any media or format and includes materials as identified by MSIPA. The categories of Covered Information under Maine law are found in Exhibit B. For purposes of this DPA, Covered Information is referred to as Student Data.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or school unit, 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 and 504 plans. The categories of Educational Records under Maine law are also found in Exhibit B. For purposes of this DPA, Educational Records are referred to as Student Data.

De-identified Data: 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.

Anonymized Data: means any Student Educational Record rendered anonymous in such a manner that the student is no longer identifiable. For example, this includes non-identifiable student assessment data and results, and other metadata, testing response times, scores (e.g. goals, RIT), NCES codes, responses, item parameters, and item sequences that result from the Services.

Operator: The term “Operator” means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. This term shall encompass the term "Third Party," as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student educational records, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by School Unit or its users, students, or students’ parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate or combination, would allow a reasonable person who does not have knowledge of the relevant circumstances to be able to identify a student. For purposes of this DPA, Personally

Identifiable Information shall include the categories of information listed in the definition of Student Data that, either alone or in aggregate or combination, would allow a reasonable person who does not have knowledge of the relevant circumstances to be able to identify a student. PII 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, provided that such anonymization and/or de-identification has been done in compliance with applicable federal law.

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA, the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by School Unit 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 School Unit employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records and Covered Information.

Service Agreement: Refers to the NWEA Master Subscription Agreement that this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by School Unit 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 Massachusetts and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools,

districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Subscribing School Unit: A School Unit 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 Agreement, the term “Subprocessor” (sometimes referred to as the “Subcontractor”) means a party other than School Unit or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

Third Party: The term “Third Party” means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term “Third Party” when used to indicate the provider of digital educational software or services is replaced by the term “Provider.”

EXHIBIT “D”

DIRECTIVE FOR DISPOSITION OF DATA

Maine School Administrative District #6 (“School Unit” directs (“Company”) to dispose of data obtained by Company pursuant to the terms of the Service Agreement between School Unit and Company. The terms of the Disposition are set forth below:

1. Extent of Disposition

___Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

___Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

___Disposition shall be by destruction or deletion of data.

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

3. Timing of Disposition

Data shall be disposed of by the following date:

___As soon as commercially practicable

___By [**Insert Date**]

4. Signature

Authorized Representative of School Unit

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT “E”

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Maine School Administrative District #6** and which is dated September 1, 2020 to any other School Unit (“Subscribing School Unit”) who accepts this General Offer through its signature below. 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 other School Unit may also agree to change the Student Data provided by School Unit to the Provider to suit the unique needs of the School Unit so long as any such Student Data is captured by the Assessment System. 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 one (1) year after the date of Provider’s signature to this Form. Provider shall notify the either the METDA or SDPC in the event of any withdrawal so that this information may be transmitted to the Alliance’s users.

Provider Name: NWEA

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

2. Subscribing School Unit

A Subscribing School Unit, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing School Unit and the Provider shall therefore be bound by the same terms of this DPA.

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

EXHIBIT “F” DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]