

EXHIBIT “H” – Additional Terms or Modifications

Version ___ NWEA _____

LEA and Provider agree to the following additional terms and modifications:

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

4. ~~This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.~~ This DPA shall stay in effect for ~~three years~~ the term of the Service Agreement unless otherwise terminated by the parties. ~~Exhibit E will expire upon expiration of termination of the Service Agreement.~~

ARTICLE IV: DUTIES OF PROVIDER

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information **that is identifiable** and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA and **in accordance with FERPA 99.33, provided that Provider will make reasonable efforts to notify LEA of such request unless prohibited by law.** Provider will not Sell Student Data to any third party.

ARTICLE V: DATA PROVISIONS

2. **Audits.** No more than once a year, or following unauthorized access, ~~upon receipt of a written request from the LEA with at least ten (10) business days’ notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA.~~ The LEA may make reasonable inquiries of the Provider regarding the use of the LEA’s Student Data and the security measures undertaken by the Provider to protect said Student Data.

The Provider will also cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider’s facilities, staff, agents and LEA’s Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit “F”**. ~~Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to Exhibit “H”.~~ Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “F”**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

EXHIBIT “C” DEFINITIONS

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians, that is descriptive of the student including, but not limited to, information

in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data **containing PII**. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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 service.

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

[INTENTIONALLY BLANK]

**EXHIBIT E IS NOT AVAILABLE
PLEASE CONTACT THE PROVIDER OR THE CSPA FOR ADDITIONAL INFORMATION.**