## EXHIBIT "H" – Additional Terms or Modifications

Version _____Microsoft_____

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

**STANDARD CLAUSES**
**Version 1.0**

**Article II, section 2, Parent Access.**
Parties agree to the revised provision:

**Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. To the extent the Provider has access to the data Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

**Article II, section 4, Law Enforcement Requests.**
Parties agree to the revised provision:

**Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request and in accordance with the provision found below.
This provision following industry standard provision from Microsoft's Data Processing Addendum ("DPA") (which is incorporated by reference in the Online Services Terms ("OST") and which is also incorporated by reference in any Microsoft agreement for Online Services):

> ***Nature of Data Processing; Ownership.*** *Microsoft will use and otherwise process Student Data only (a) to provide Online Services in accordance with the LEA's documented instructions, and (b) for Microsoft's legitimate business operations, each as detailed and limited below. As between the parties, the LEA retains all right, title and interest in and to Student Data. Microsoft acquires no rights in Student Data, other than the rights the LEA grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to the LEA.*
>
> ***Disclosure of Processed Data.*** *Microsoft will not disclose Processed Data except: (1) as the LEA directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Personal Data; and (c) any other data processed by Microsoft in connection with the Online Service that is the LEA's confidential information under the volume license agreement. All processing of Processed Data is subject to Microsoft's obligation of confidentiality under the volume license agreement.*

*Microsoft will not disclose Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from the LEA. If compelled to disclose Processed Data to law enforcement, Microsoft will promptly notify the LEA and provide a copy of the demand unless legally prohibited from doing so.*

*Upon receipt of any other third-party request for Processed Data, Microsoft will promptly notify the LEA unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from the LEA.*

*Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform F keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.*

*In support of the above, Microsoft may provide the LEA's basic contact information to the third party.*

**Article IV, Section 5**
Parties agree to the revised provision:

**De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless ~~(a)~~ that party agrees in writing not to attempt re-identification.~~, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer.~~ Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

**Article V, section 2**

**Audits**
Parties agree to the revised provision:

**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.

> *In accordance with the above, Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data and Personal Data, as follows:*
>
> *Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.*
> *Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.*
> *Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.*
> *Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which Microsoft will make available at https://servicetrust.microsoft.com/ or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor. If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.*
>
> *To the extent Customer's audit requirements under the Standard Contractual Clauses or Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers, Microsoft will promptly respond to Customer's additional audit instructions. Before the commencement of an audit, Customer and Microsoft will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Microsoft to unreasonably delay performance of the audit. To the extent needed to perform the audit, Microsoft will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data and Personal Data by Microsoft, its Affiliates, and its Subprocessors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Microsoft, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Microsoft's other customers or to Microsoft systems or facilities not involved in the Online Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Microsoft expends for any such audit, in addition to the rates for services performed by Microsoft. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Microsoft and Microsoft shall promptly cure any material non-compliance.*
>
> *If the Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses. Nothing in this section of the DPA varies or modifies the Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses or Data Protection Requirements. Microsoft Corporation is an intended third-party beneficiary of this section.*

**Article V, section 3, <u>Data Security.</u>**

(Add below to Exhibit F)

Parties agree that the following further documentation on Microsoft's security commitments will apply and are incorporated into the contract via the Online Services Privacy & Security Terms, inclusive of the Data Protection Addendum, found at : <u>Commercial Licensing Terms (microsoft.com)</u>.

**Article V, section 4, Data Breach.**
Parties agree to the revised provision:

**Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

~~(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:~~

~~i. The name and contact information of the reporting LEA subject to this section.~~
~~ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.~~
~~iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.~~
~~iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and~~
v. ~~A general description of the breach incident, if that information is possible to determine at the time the notice is provided.~~

***Security Incident Notification***. *If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Student Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify the LEA of the Security Incident; (2) investigate the Security Incident and provide the LEA with detailed information about the Security Incident; in accordance with applicable state law (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.*

*Notification(s) of Security Incidents will be delivered to one or more of the LEA's administrators ~~by any means Microsoft selects, including~~ via email. It is the LEA's sole responsibility to ensure the LEA's administrators maintain accurate contact information on each applicable Online Services portal. The LEA is solely responsible for complying with its obligations under incident notification laws applicable to the LEA and fulfilling any third-party notification obligations related to any Security Incident.*

*Microsoft shall make reasonable efforts to assist the LEA in fulfilling the LEA's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.*

*Microsoft's notification of or response to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.*

*The LEA must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.*

(2) Provider agrees to adhere to all federal and state requirements 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 data breach.

(3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## EXHIBIT "E"

### GENERAL OFFER OF PRIVACY TERMS

**1**. **Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and Oak Grove School District ("Originating LEA") which is dated Nov 11, 2021, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("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 Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

Jai.Dhir@microsoft.com

**PROVIDER:** Microsoft Corporation

BY: Beth Dann Date: 11-12-2021

Printed Name: Beth Dann Title/Position: General Manager West-US Education

**2**. **Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Oak Grove School District and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

**LEA:** San Mateo County Office of Education

BY: Lorrie Owens Date: 11-03-2022

Printed Name: Lorrie Owens Title/Position: Chief Techology Officer,

SCHOOL DISTRICT NAME: San Mateo County Office of Education Information Technology

DESIGNATED REPRESENTATIVE OF LEA:

Name: Lorrie Owens

Title: Chief Techology Officer, Information Technology

Address: 101 Twin Dolphin DriveRedwood CityCalifornia94065

Telephone Number: 650-802-5300

Email: lowens@smcoe.org