

Amendment to Contract Documents

Agreement Number

01C35680

000-arlened-E-240

This amendment ("Amendment") is entered into between the parties identified on the attached program signature form. It amends the Enrollment or Agreement identified above. All terms used but not defined in this Amendment will have the same meanings provided in that Enrollment or Agreement.

Campus and School Agreement Custom Terms CTM

This Amendment has been reviewed by the California Educational Technology Professional Association ("CETPA") and its counsel. They have determined that this Amendment complies with Federal and California privacy law, including FERPA and AB 1584.

The parties agree that the Agreement is amended as follows:

A) Use of Customer Data

Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer.

B) Security

Microsoft is committed to helping protect the security of Customer's information. Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

Security Training. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.

C) Educational Institutions

If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA) apply, Microsoft acknowledges that for the purposes of the OST, Microsoft is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials.

Customer understands that Microsoft may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Microsoft to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Microsoft's possession as may be required under applicable law.

D) Data Retention

At all times during the term of Customer's subscription, Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials, which customer or Microsoft will delete per the terms of the trial software, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. During this period, Microsoft provides multiple notices, so you will be amply forewarned of the upcoming deletion of data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data.

E) Third-party Users

Third-party users of Customer's services have no privity of contract with Microsoft, and must exercise their rights to their own data that may be contained in Customer Data by working directly with Customer. Any third-party seeking to enforce their rights to their own data contained in Customer Data may retain possession and control of their own third-party generated content and may review personally identifiable information and correct erroneous information, by requesting Customer staff assist them in obtaining possession and control, and/or in reviewing/correcting content/information.

F) Parent Access and Student Accounts

Customer shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information in the pupils records, correct erroneous information, and procedures for the transfer of pupil generated content to a personal account, consistent with the functionality of services. Customer shall be responsible for administering this process. During the term of the enrollment, Microsoft shall maintain access to the data the customer wishes to modify or delete. In the event that Microsoft is contacted by an individual seeking access to personal identifiable information, Microsoft shall, where feasible, refer the individual to the customer, who will follow the necessary and proper procedures regarding the requested information.

G) Security Incident Notification

If Microsoft becomes aware of any unlawful access to any Customer Data or Support Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data or Support Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident, including, if known, the date or estimated date of the unlawful access and the categories of data affected; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. Given the nature of the Online Services and Microsoft's privacy policies, Microsoft will generally not have knowledge of the data or categories of data stored by Customer. In the event of

unlawful access, Microsoft's ability to provide detailed information about the data accessed may be limited. Microsoft will provide such details about the unlawful access as are reasonably available to it.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

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

H) Applicable Law, Venue and Jurisdiction

This agreement is governed by the laws of the State of California. The parties agree that any lawsuits that include a claim for money damages against Institution relating to this agreement must be brought in the United States District Court, Southern Division, located in Santa Ana, California. Any other legal actions relating to this agreement must be brought in a court of competent jurisdiction within federal courts located in the jurisdiction of the state where Institution is organized, and the parties agree that jurisdiction and venue in such courts is appropriate, where prerequisites for federal court jurisdiction are present.

I) Subcontractor Transfer.

Microsoft may hire subcontractors to provide certain limited or ancillary services on its behalf. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the DPT. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the DPT. Except as set forth in the DPT, or as Customer may otherwise authorize, Microsoft will not transfer to any third party (not even for storage purposes) personal data Customer provides to Microsoft through the use of the Online Services. Microsoft provides a website that lists subcontractors authorized to access Customer Data in the Online Services as well as the limited or ancillary services they provide. At least 6 months before authorizing any new subcontractor to access Customer Data, Microsoft will update the website and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent Customer invoices.

J) Online Services Information Security Policy

Each Online Service follows a written data security policy ("Information Security Policy") that complies with the control standards and frameworks shown in the table below.

Online Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Office 365 Services	Yes	Yes	Yes	Yes	Yes
Microsoft Dynamics 365 Core Services	Yes	Yes	Yes	Yes*	Yes*
Microsoft Azure Core Services	Yes	Yes	Yes	Varies**	Varies**
Microsoft Cloud App Security	Yes	Yes	Yes	Yes	Yes
Microsoft Graph	Yes	Yes	Yes	No	No
Microsoft Intune Online Services	Yes	Yes	Yes	Yes	Yes
Microsoft Business Application Platform Core Services	Yes	Yes	Yes	Yes	Yes

**Does not include Microsoft Social Engagement.*

***Current scope is detailed in the audit report and summarized in the Microsoft Azure Trust Center.*

Microsoft will provide an updated schedule for products not shown on this graph via the Online Services Terms document.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate a standard or framework in the table above unless it is no longer used in the industry and it is replaced with a successor (if any). In the event Microsoft provides Customer with products not shown on the schedule above, Microsoft, where appropriate, will provide an updated schedule listing the Microsoft product or service and the applicable control standard via the Online Services Terms document.

Subject to non-disclosure obligations, Microsoft will make each Information Security Policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.

Customer is solely responsible for reviewing each Information Security Policy and making an independent determination as to whether it meets Customer's requirements.

K) General Offer of Privacy Terms.

Microsoft offers the same privacy protections found in this Amendment between it and Customer to any other local education agency ("LEA") in California who accepts this General Offer through its signature on a separate form. This General Offer shall extend only to privacy protections, and Microsoft's signature shall not necessarily bind Microsoft to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this Amendment. Microsoft and the subscribing LEA may also agree to change the data provided by LEA to Microsoft to suit the unique needs of the LEA. Microsoft 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 listed in the Originating Service Agreement; or three (3) years after the date of Microsoft's signature to the General Offer. Microsoft shall notify the California Student Data Privacy Alliance in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Except for changes made by this Amendment, the Enrollment or Agreement identified above remains unchanged and in full force and effect. If there is any conflict between any provision in this Amendment and any provision in the Enrollment or Agreement identified above, this Amendment shall control.

This Amendment must be attached to a signature form to be valid.

Microsoft Internal Use Only:

CTM - CASA	CTM	CTM-CTC-AGR	BD
------------	-----	-------------	----