Campus and School Agreement
Custom Terms CTM

The parties agree that the Agreement is amended as follows, in accordance with Louisiana Revised Statute 17:3914:

A) Customer Data

Customer Data for the purposes of this agreement is deemed to mean all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. This includes student information and personally identifiable information.

B) 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 or for any other purpose other than agreed to herein. 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.

C) Disclosure of Customer Data and Support Data

Microsoft will not disclose Customer Data or Support Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in the OST, or (3) as required by law.

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

Upon receipt of any other third-party request for Customer Data or Support Data, Microsoft will promptly notify Customer 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 Customer.

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

Unless required by law, Microsoft will not share any data under this agreement without prior written approval for any purpose not expressly permitted in this Agreement. Microsoft cannot disclose any document, whether in hard copy or electronic form, or otherwise disclose to any third party any student-level data or information in any form whatsoever or under any circumstances which would directly or indirectly makes a student's identity easily traceable.

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

D) 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 Measures. *The Online Services Terms addresses Data Security Practices and Policies and is updated monthly. Microsoft may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the security of the Services.*

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.

Access to physical datacenter facilities is guarded by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, multifactor access control, integrated alarm systems, and around-the-clock video surveillance by the operations center.

Virtual access to customer data is restricted based on business need by role-based access control, multifactor authentication, minimizing standing access to production data, and other controls. Access to customer data is also strictly logged, and both Microsoft and third parties perform regular audits (as well as sample audits) to attest that any access is appropriate.

E) **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.

F) **Data Retention and deletion**

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, 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. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data.

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; and (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 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) **Microsoft Audits of Online Services**

For each Online Service, at the request of the State or its authorized representative, Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data). The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

Microsoft will automatically conduct such audits as follows:

• Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each Online Service.

• 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 will be Microsoft's Confidential Information. The Microsoft Audit Report 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.

The list of available audit/compliance reports can be found here:
https://servicetrust.microsoft.com/Documents/ComplianceReports

I) **Business Continuity Management**

Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data are located.

Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

J) **Location of Customer Data at Rest**

Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as follows:

- **Office 365 Services.** If Customer provisions its tenant in the United States Microsoft will store the following Customer Data at rest only within the United States (specified Geo) (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, and Project Online data, and (3) files uploaded to OneDrive for Business.
- **Microsoft Intune Online Services**. When Customer provisions a tenant account, Customer selects an available Geo where Customer Data at rest will be stored. Microsoft will not transfer the Customer Data outside of Customer's selected Geo except as noted in the "Data Location" section of the Microsoft Intune Trust Center.
- **Microsoft Business Application Platform Core Services**. If Customer provisions its tenant in the United States, Microsoft will store Customer Data at rest only within the United States, except as noted in the data location section of the Microsoft Business Application Platform Trust Center.
- **Microsoft Azure Core Services**. If Customer configures a particular service to be deployed within a Geo then, for that service, Microsoft will store Customer Data at rest within the specified Geo. Certain services may not enable Customer to configure deployment in a particular Geo or outside the United States and may store backups in other locations, as detailed in the Microsoft Azure Trust Center (which Microsoft may update from time to time, but Microsoft will not add exceptions for existing Services in general release).
- **Microsoft Cloud App Security**. Microsoft will store Customer Data at rest in the United States.
- **Microsoft Dynamics 365 Core Services**. Except for Microsoft Social Engagement, and only for entities managed by the Microsoft Dynamics 365 Core Services, if Customer provisions its instance of Microsoft Dynamics 365 Core Services in the United States, Microsoft will store Customer Data at rest within the specified Geo. Certain entities may not be configured to be stored in any particular Geo and may be stored at rest in other locations as detailed in the Microsoft Dynamics 365 Trust Center.

Microsoft does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.