Microsoft Volume Licensing

Amendment to Contract Documents
Campus and School Agreement
Custom Terms Amendment

Agreement Number	01C36218	01C36218-06292020

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.

This amendment hereby replaces Amendment # 01C36218-08222019-2 in its entirety.
For clarity, 01C36218-08222019-1 remains in full force and effect.

The following section entitled "Data Sharing and Confidentiality Agreement" is hereby added to the Agreement as follows:

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

AND

SUPPLEMENTAL INFORMATION TO THE AGREEMENT

1. **Purpose**

WHEREAS, a Board of Cooperative Educational Services ("BOCES") is a municipal corporation organized and existing under the Education Law of the State of New York that pursuant to Education Law §1950 provides shared computer services and software to school district components ("District" or "Districts") of the Regional Information Center ("RIC") and in that capacity purchases various products for use by said districts as part of the BOCES service;

WHEREAS, Erie 1 BOCES is also responsible for negotiating and entering into technology contracts and that other BOCES may bind themselves to such contracts and allow for the purchase of services under such contracts by adopting appropriate School Board resolutions.

WHEREAS Erie 1 BOCES and Microsoft entered into and have been operating under the Campus and School Agreement ("Agreement");

WHEREAS, several BOCES throughout New York State have been bound to, are allowing for the purchase of services under, and will continue to allow for the purchase of services under the Agreement;

WHEREAS, the Agreement is subject to the New York's Education Law Section 2-d ("Education Law 2-d"); and

WHEREAS, Parties wish to amend the Agreement so as to be compliant with the Education Law 2-d and Microsoft agrees to abide by the following terms in accordance with Microsoft's Online Services Terms ("OST").

NOW, THEREFORE, in consideration of the foregoing recitals and the mutual covenants contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereto agree as follows:

2. **Definitions**

Any capitalized term used within this Amendment that is also found in the Agreement will have the same definition as contained within the Agreement.

In addition, as used in this Amendment:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the Agreement.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the Agreement.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the Agreement. For purposes of this Amendment, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the Agreement to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Agreement may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d). Vendor's data security and privacy plan for how all state, federal and local data security and privacy contract requirements will be implemented over the term of this Agreement is as follows:

Microsoft has implemented and will maintain for Customer Data, which includes Shared Data as defined in this Agreement, in the Core Online Services the following security measures, which, in conjunction with the security commitments in the OST (including the GDPR Terms), are Microsoft's only responsibility with respect to the security of that data.

Domain	Practices
Organization of Information Security	**Security Ownership.** Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities.** Microsoft personnel with access to Customer Data are subject to confidentiality obligations. **Risk Management Program.** Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory.** Microsoft maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. **Asset Handling** - Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities.
Human Resources Security	**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.

Domain	Practices
Physical and Environmental Security	**Physical Access to Facilities**. Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals. **Physical Access to Components**. Microsoft maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain. **Protection from Disruptions**. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered. - Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. - Microsoft has specific procedures in place governing access to copies of Customer Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services, which are reviewed every twelve months. - Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries** - Microsoft encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. - Microsoft restricts access to Customer Data in media leaving its facilities. **Event Logging**. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Microsoft ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data when needed. - Microsoft restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. - Microsoft stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data are located.

Domain	Practices
	- 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.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Amendment, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the Agreement, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the Agreement: See Section 3(b) above.

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information in the Agreement" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor [*check one*] _X_____will _____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the Agreement and agrees to be responsible for their performance subject to the terms of the Agreement and this Amendment. The list of subcontractors is located at: https://www.microsoft.com/en-us/trust-center/privacy/data-access#subcontractors

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Amendment.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the Agreement is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the Agreement and the terms of this Amendment:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the Agreement.

(c) Not use education records for any purposes other than those explicitly authorized in this Amendment.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the Agreement, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Amendment) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, and and Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security

Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

ERIE 1 BOCES

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Erie 1 BOCES is committed to protecting the privacy and security of personally identifiable information about students who attend Erie 1 BOCES instructional programs in accordance with applicable law, including New York State Education Law Section 2-d.

To further these goals, Erie 1 BOCES wished to inform parents of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

SUPPLEMENTAL INFORMATION

ABOUT THE AGREEMENT

BETWEEN

ERIE 1 BOCES AND MICROSOFT

Erie 1 BOCES has entered into a Campus and School Agreement ("Agreement") with [*MICROSOFT*] which governs the availability to Participating Educational Agencies of the following Product(s):

Online Services	
Microsoft Dynamics 365 Core Services	The following services, each as a standalone service or as included in a Dynamics 365 branded plan or application: Dynamics 365 Customer Service Enterprise, Dynamics 365 Customer Service Professional, Dynamics 365 Customer Service Insights, Dynamics 365 Field Service, Dynamics 365 Business Central, Dynamics 365 Supply Chain Management, Dynamics 365 Finance, Dynamics 365 Marketing, Dynamics 365 Project Service Automation, Dynamics 365 Commerce, Dynamics 365 Human Resources, Dynamics 365 Sales Enterprise, and Dynamics 365 Sales Professional. Dynamics 365 Core Services do not include (1) Dynamics 365 Services for supported devices or software, which includes but is not limited to Dynamics 365 for apps, tablets, phones, or any of these; (2) LinkedIn Sales Navigator; or (3) except as expressly defined in the licensing terms for the corresponding service, any other separately-branded service made available with or connected to Dynamics/365 Core Services.
Office 365 Services	The following services, each as a standalone service or as included in an Office 365-branded plan or suite: Compliance Manager, Customer Lockbox, Exchange Online Archiving, Exchange Online Protection, Exchange Online, Microsoft Bookings, Microsoft Forms, Microsoft MyAnalytics, Microsoft Planner, Microsoft StaffHub, Microsoft Stream, Microsoft Teams (including Bookings, Lists, and Shifts), Microsoft To-Do, Office 365 Advanced Threat Protection, Office 365 Video, Office for the web, OneDrive for Business, Project (except Roadmap and Project for the web), SharePoint Online, Skype for Business Online, Sway, Whiteboard, Yammer Enterprise and, for Kaizala Pro, Customer's organizational groups managed through the admin portal and chats between two members of Customer's organization. Office 365 Services do not include Office 365 ProPlus, any portion of PSTN Services that operate outside of Microsoft's control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded "for Office 365."
Microsoft Azure Core Services	API Management, App Service (API Apps, Logic Apps, Mobile Apps, Web Apps), Application Gateway, Application Insights, Automation, Azure Active Directory, Azure Cache for Redis, Azure Container Registry (ACR), Azure Container Service, Azure Cosmos DB (formerly DocumentDB), Azure Database for MySQL, Azure Database for PostgreSQL, Azure Databricks, Azure DevOps Services, Azure DevTest Labs, Azure DNS, Azure Information Protection (including Azure Rights Management), Azure Kubernetes Service, Azure NetApp Files, Azure Resource Manager, Azure Search, Backup, Batch, BizTalk Services, Cloud Services, Computer Vision, Content Moderator, Data Catalog, Data Factory, Data Lake Analytics, Data Lake Store, Event Hubs, Express Route, Face, Functions, HDInsight, Import/Export, IoT Hub, Key Vault, Load Balancer, Log Analytics (formerly Operational Insights), Azure Machine Learning Studio, Media Services, Microsoft Azure Portal, Multi-Factor Authentication, Notification Hubs, Power BI Embedded, QnA Maker, Scheduler, Security Center, Service Bus, Service Fabric, Site Recovery, SQL Data Warehouse, SQL Database, SQL Server Stretch Database, Storage, StorSimple, Stream Analytics, Text Analytics, Traffic Manager, Virtual Machines, Virtual Machine Scale Sets, Virtual Network, and VPN Gateway
Microsoft Cloud App Security	The cloud service portion of Microsoft Cloud App Security.
Microsoft Intune Online Services	The cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune such as Mobile Device Management for Office 365.
Microsoft Power Platform Core Services	The following services, each as a standalone service or as included in an Office 365 or Microsoft Dynamics 365 branded plan or suite: Microsoft Power BI, Microsoft Power Apps, and Microsoft Power Automate. Microsoft Power Platform Core Services do not include any client software, including but not limited to Power BI Report Server, the Power BI, PowerApps or Microsoft Power Automate mobile applications, Power BI Desktop, or Power Apps Studio.
Microsoft Defender Advanced Threat Protection Services	The following cloud service portions of Microsoft Defender Advanced Threat Protection: Attack Surface Reduction, Next Generation Protection, Endpoint Detection & Response, Auto Investigation & Remediation, Threat & Vulnerability Management, SmartScreen.

Pursuant to the Agreement, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the Agreement. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the Agreement (including any hosting service provider). Vendor will ensure that such subcontactors, assignees, or other authorized agents

abide by the provisions of these agreements and is responsible for their performance under the agreement.

Duration of Agreement and Protected Data Upon Expiration:

- The Agreement commenced on July 30, 2013 and has no expiration date.

- Upon expiration of any Enrollment under this Agreement without renewal, Vendor shall, if requested by BOCES, or Participating Educational Agency, provide tools to the BOCES, or Participating Educational Agency for exporting all electronically stored Shared Data previously received back to the BOCES or Participating Educational Agency. Microsoft will retain the Protected Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of this Agreement. Thereafter, Vendor shall promptly securely delete and/or dispose of any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors (including all electronic versions or electronic imaging of hard copies of Protected Data) unless Microsoft is required by applicable law to retain such data. Vendor agrees that neither it nor its subcontractors or assignees will retain any copy, summary or extract of the Protected Data or any related work papers on any storage medium whatsoever unless Microsoft is required by applicable law to retain such data. Upon request, Vendor and/or its subcontractors or assignees will provide a certification from an appropriate officer that the requirements of this paragraph have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

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:

Erie 1 CASA Amendment (NYS Ed-2d -PBOR v2) 06262020.docx	CTM	CTM-CTC-LOL-AGR	BD

Microsoft Volume Licensing

Alternative Acceptance Form (Microsoft Only)

Due to the extraordinary impact of the coronavirus (COVID-19), Microsoft has implemented steps to protect personnel and the communities in which they live and work, including conducting business from remote locations and/or using different processes. As a result, Microsoft is utilizing this Alternative Acceptance Form in place of signing a Program Signature Form.

Microsoft's authorized representative is accepting the contract documents shown on the Program Signature Form bearing the Proposal ID shown below ("Contract Documents") by typing their name and entering the date of acceptance on this Alternative Acceptance Form. The Agreement Effective Date shown below is the Agreement Effective Date shown on the Program Signature Form.

For the purposes of this Alternative Acceptance Form, "Customer" means the Customer entity identified on the Program Signature Form bearing the same Proposal ID that appears on this form, and "Microsoft" means the Microsoft entity or entities identified below on this form.

MBA/MBSA number:	
Agreement number:	01C36218
Enrollment number:	
Proposal ID:	CTM (01C36218)
Opportunity ID (if applicable):	01C36218-06292020
Agreement Effective Date:	
Customer Name:	Erie 1 BOCES

To indicate Microsoft's agreement, Microsoft's duly authorized representative will complete this form by entering their name and the date of Microsoft's acceptance below. Upon completion of this form, Microsoft agrees that it (1) has received, read and understands this Alternative Acceptance Form, the Program Signature Form, and all Contract Documents, including any websites or documents incorporated by reference and any amendments, and (2) agrees to be bound by the terms of all such documents, as of the Agreement Effective Date. This Alternative Acceptance Form, when completed, will be incorporated into the Agreement noted above.

Acceptance by Microsoft	
Enter applicable Microsoft Affiliate: Microsoft Corporation	
Name of Microsoft authorized representative:	Shirley Snyder Customer Care Specialist
Acceptance date:	June 29, 2020
The above person is duly authorized on behalf of Microsoft to accept these Contract Documents. Microsoft will not challenge the enforceability or validity of the agreement formed by this alternative process or any of the Contract Documents based on its acceptance using this Alternative Acceptance Form.	

Optional Confirmation of Acceptance on Customer Request

Once Microsoft returns to its normal business processes, if Customer requests a Microsoft signature, an authorized representative of Microsoft will sign and deliver a copy of this Alternative Acceptance Form below to confirm the effectiveness of the agreement as of the Agreement Effective Date shown above.

Optional Microsoft Confirmation of Acceptance	
Enter applicable Microsoft Affiliate: <choose one>	
By signature of its duly authorized representative below, Microsoft hereby acknowledges, ratifies and confirms that the agreement referenced on this Alternative Acceptance Form was duly accepted, and is effective as of the Agreement Effective Date shown above.	
Signature:	**sign your complete name**
Printed First and Last Name:	**print your complete name**
Printed Title:	**print your title**
Signature Date:	**enter the date you signed this form**