Amendment to Campus and School Agreement

This Amendment to the Campus and School Agreement (the "**Amendment**") is made and entered into as of the 22nd day of August, 2019, by and between Microsoft Corporation and its subsidiaries ("**Microsoft**" or "**Vendor**") and Erie 1 Board of Cooperative Educational Services ("**Erie 1 BOCES**")(each a "**Party**" and, collectively, the "**Parties**").

RECITALS:

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:

The following definitions apply to the terms of this Amendment:

"**Eligible Student**" means a student eighteen years or older.

"**Parent**" means a parent, legal guardian, or person in parental relation to a student.
"Product" means all products identified on the Product List, such as software, Online Services and other web-based services, including pre-release or beta versions;

"**Shared Data**" means collectively Student Data, Teacher/Principal Data and PPSI.

"Student" means any person attending or seeking to enroll in a school district or BOCES purchasing Microsoft products pursuant to the Campus Agreement.

"Student Data" means personally identifiable information from student records of any Student.

"Teacher/Principal Data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is

confidential and not subject to release under the provisions of section three thousand twelve-c of New York Education Law.

"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

"Personal, Private, and Sensitive Information" ("PPSI") is any information to which unauthorized access, disclosure, modification, destruction, or disruption of access or use could severely impact critical functions, employees, customers or third parties, or students in general. Private information could include one or more of the following: Social Security number; driver's license number or non-driver ID; account number, credit card number, or debit card number and security code; or access code/password that permits access to an individual's financial account or protected student records.

1.1. Product shall be utilized at the sites as shall be designated by BOCES or District, or utilized in a cloud environment and shall be used solely for the benefit of BOCES or such licensed component District. BOCES or a licensed component District shall not permit or provide for transfer or reproduction of Product, or any portion thereof, to be placed on a computer not at the sites, by physical or electronic means, unless specifically authorized. BOCES, or a licensed component District, shall not make or allow others to make copies or reproductions of the Product, or any portion thereof in any form without the prior written consent of Vendor. The unauthorized distribution or disclosure of the Product, is prohibited, and shall be considered a material breach of the Agreement.

1.2. Except as expressly stated herein, BOCES, or a licensed component District, may not alter, modify, or adapt the Product, including but not limited to translating, reverse engineering, decompiling, disassembling, or creating derivative works, and may not take any other steps intended to produce a source language state of the Product or any part thereof, without Vendor's prior express written consent.

1.3. BOCES, or a licensed component District, will be the sole owner and custodian of data transmitted, received, or manipulated by the Product, except as otherwise set forth in this Agreement.

In the event that Vendor stores or maintains Shared Data provided to it by a BOCES, RIC or licensed component district, whether as a cloud provider or otherwise, the Vendor assumes all risks and obligations in the event of a breach of security of such data where such breach of security is caused solely by Vendor's gross negligence or willful misconduct. Vendor may subcontract or assign its obligation to store or maintain Shared Data provided to it pursuant to this Agreement to a third party cloud provider so long as Microsoft remains responsible for such third party's performance and compliance with all the terms of this Agreement including, but not limited to, compliance with the training provisions of this Agreement.

So long as a BOCES, RIC or District provisions its data center in the United States of America, Shared Data transferred to Vendor by a BOCES, RIC or a District will be stored in electronic format on systems maintained by Vendor in a secure data center facility located within the United States of America. The measures that Vendor will take to protect the privacy and security of the Shared Data while it is stored in that manner are those associated with industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection as outlined in Microsoft's Security Practices and Policies that has been incorporated within this Agreement.

Vendor must promptly inform the BOCES, RIC or licensed component district, as applicable, in the event that any Shared Data it stores or maintains pursuant to this Agreement, including such data as may be stored or maintained by a third party cloud provider on Vendor's behalf, is requested by law enforcement authorities or otherwise sought by subpoena or court order.

Vendor will keep confidential all information and data, including any Shared Data to which it has access in the performance of this Agreement.

In addition to the above requirements, for Shared Data as defined above:

1) Vendor shall maintain the confidentiality of the Shared Data in accordance with applicable state and federal law. Microsoft agrees to act in good faith to modify the terms of this Amendment if the Education Law 2-d is updated..

2) 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.
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.

Domain	Practices
	- 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. - 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.

3) Vendor's data security and privacy Plan includes Erie 1 BOCES' Parents Bill of Rights for data privacy and security (a copy of which is attached hereto and incorporated into this Agreement as **Exhibit A**).

4) In accordance with Vendor's data security and privacy Plan, Vendor agrees that any of its officers or employees, and any officers or employees of any subcontractor or assignee of Vendor, who will have access to the Shared Data, have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving the data or access to the data. Upon request, Vendor will make an audit report available in the Microsoft Trust Center to show. that the requirements of this paragraph have been satisfied in full.

5) The exclusive purposes for which Vendor is being provided access to the Shared Data is:

Processing of Customer Data; Ownership

Customer Data, which includes Shared Data as defined in this Agreement, will be used or otherwise processed only to provide Customer or Districts the Online Services including purposes compatible with providing those services. Microsoft will not use or otherwise process 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. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

6) Vendor will ensure that it will only share Shared Data with additional third parties if those third parties are contractually bound to observe the same obligations to maintain data privacy and security as required by Vendor pursuant to this Agreement.

7) Upon expiration of this Agreement without renewal, Vendor shall, if requested by BOCES, RIC or a licensed component district, provide tools to the BOCES, RIC or the licensed component district for exporting all electronically stored Shared Data previously received back to the BOCES, RIC or a licensed component district. , Microsoft will retain the Shared 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 Shared Data remaining in the possession of Vendor or its assignees or subcontractors (including all electronic versions or electronic imaging of hard copies of Shared 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 Shared 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.

8) In the event that a Parent or Eligible Student wishes to challenge the accuracy of the Shared Data concerning that Student or Eligible Student that is maintained by Vendor, that challenge may be processed through the procedures provided by the licensed component district for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Vendor will be notified by the licensed component district of the outcome of any such challenges and promptly correct any inaccurate data it or its subcontractors or assignees maintain. A teacher or principal who wishes to challenge the accuracy of the Shared Data concerning that teacher or principal that is maintained by Vendor may do so through the process set forth in the APPR plan of their employing school district or BOCES.

9) Shared Data transferred to Vendor by a BOCES, RIC or a licensed component district will be stored in electronic format on systems maintained by Vendor in a secure data center facility located within the United States of America. The measures that Vendor will take to protect the privacy and security of the Shared Data while it is stored in that manner are those associated with industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

10) Shared Data received by Vendor or by any subcontractor or assignee of Vendor from a BOCES, RIC or a licensed component district shall not be sold or released for any commercial purposes, nor shall it be sold or used for marketing purposes.

11) Vendor acknowledges that it has the following additional obligations under NYS Education Law 2-d with respect to any Shared Data received from a BOCES, RIC or a licensed component district, and agrees that any failure to fulfill one or more of these statutory obligations shall be deemed a breach of this Agreement, as well as subject Vendor to various penalties under Education Law 2-d, including but not limited to civil penalties:

    a. To limit internal access to education records and Student Data 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); *e.g.,* the individual needs access to the Student Data in order to fulfill his or her responsibilities in performing the services provided to a BOCES, RIC or a licensed component district by Vendor;

    b. To not use education records or Shared Data for any purpose(s) other than those explicitly authorized in this Agreement;

    c. To not disclose any personally identifiable information to any other party who is not an authorized representative of Vendor using the information to carry out Vendor's obligations under this 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 the BOCES, RIC or a licensed component district prior to the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

    d. To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;

    e. To use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2), or any other technology or methodology specifically authorized by applicable statute, regulation or the NYS Education Department;

    f. To notify the applicable BOCES, RIC and District of any breach of security resulting in an unauthorized release of such data by Vendor or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for student data privacy and security and obligations relating to data privacy and security within this Agreement in the most expedient way possible and without unreasonable delay.

12) In the event that a BOCES, RIC or a District is required under Education Law 2-d to notify Parent(s) or Eligible Student(s) of an unauthorized release of Shared Data by Vendor or its assignees or subcontractors, Vendor shall promptly reimburse the BOCES, RIC or a licensed component district for the full cost of such notification. Microsoft will also be responsible for the cost of provisioning one year of credit monitoring service to all affected individuals. The cost of such notification and credit monitoring shall be considered direct damages and shall not be subject to the limitations of liabilities limitations including in this Agreement.

1.4. BOCES, or a licensed component District, shall keep confidential the Product and all Documentation associated therewith whether or not protected by copyright. BOCES, or a licensed component District, will reasonably protect such information and at a minimum provide

the same safeguards afforded its own like confidential information. Confidential information shall not include information in the public domain, information already rightfully in the possession of the other party without an obligation to keep it confidential, information obtained from another source without obligations of confidentiality, information independently developed, or information required to be disclosed by a court or government order or applicable law.

1.5. Vendor shall have the right upon, three business days written notice to BOCES or a licensed component district, as applicable, to enter the premises of the BOCES or the component District for the purpose of inspecting to ensure compliance by the BOCES or the component district of its obligations hereunder. Entry shall only be allowed Monday through Friday during the normal business hours or 8:00 A.M. to 3:00 P.M. Eastern Time.

1.6. To the extent that any term of Microsoft's OST directly conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

Exhibit A

Parents' Bill of Rights for Data Privacy and Security

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community 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.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx 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 directed to the Chief Privacy Officer via email at: CPO@mail.nysed.gov.

Supplemental Information About Third Party Contractors

In the course of complying with its obligations under the law and providing educational services, Erie 1 BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law.

Each contract the BOCES enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

(1) the exclusive purposes for which the student data or teacher or principal data will be used;

(2) how the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

(3) when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

(4) if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

(5) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.