

**DATA PRIVACY AND SECURITY
MEMORANDUM OF AGREEMENT**

WHEREAS, Zoom Video Communications, Inc., having its offices at 55 Almaden Boulevard, 6th Floor, San Jose, California 95113 (hereinafter “Contractor” or “Zoom”) and the Board of Cooperative Educational Services, Second Supervisory District of Erie, Chautauqua and Cattaraugus Counties, having its offices at 8685 Erie Road, Angola, New York 14006 (hereinafter “E2CCB”), collectively “the Parties,” are parties to an agreement with an effective date of July 1, 2019 (hereinafter the “Master Agreement”) through which Contractor will provide video communications services; and

WHEREAS, pursuant to the Master Agreement, Contractor will receive student data and/or teacher or principal data in possession of E2CCB and/or its officers, employees, agents, and students, and may also receive student data and/or teacher or principal data of educational agencies within New York State that contract with E2CCB for the use of Zoom’s video communications services; and

WHEREAS, in entering into this Memorandum of Agreement (hereinafter “MOA”) the Parties seek to amend the terms of that Master Agreement in conformance with N.Y. Education Law § 2-d and 8 N.Y.C.R.R. § 121.1, *et seq.*

NOW, THEREFORE, the Parties mutually agree that the Master Agreement is hereby amended as follows:

1. For purposes of this MOA, terms shall be defined as follows:
 - a. “Breach” means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.
 - b. “Commercial Purpose” or “Marketing Purpose” means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.
 - c. “Disclose” or “Disclosure” means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.
 - d. “Education Records” means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
 - e. “Eligible Student” means a student who is eighteen years or older.

- f. “Encryption” means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.
 - g. “Parent” means a parent, legal guardian, or person in parental relation to a student.
 - h. “Personally Identifiable Information,” as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in N.Y. Education Law §3012-c (10).
 - i. “Release” shall have the same meaning as Disclosure or Disclose.
 - j. “Student” means any person attending or seeking to enroll in an educational agency.
 - k. “Student data” means personally identifiable information from the student records of an educational agency. For purposes of this agreement, “student data” includes information made accessible to Contractor by E2CCB, E2CCB officers, E2CCB employees, E2CCB agents, E2CCB students, and/or the officers, employees, agents, and/or students of educational agencies with whom E2CCB contracts.
 - l. “Teacher or 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 N.Y. Education Law §§ 3012-c and 3012-d. For purposes of this agreement, “student data” includes information made accessible to Contractor by E2CCB, E2CCB officers, E2CCB employees, E2CCB agents, E2CCB students, and/or the officers, employees, agents, and/or students of educational agencies that contract with E2CCB in order to access Contractor’s services.
 - m. “Unauthorized Disclosure” or “Unauthorized Release” means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.
2. Contractor agrees that the security, confidentiality, and integrity of student data and/or teacher or principal data shall be maintained in accordance with:
- a. Applicable state and federal laws that protect the confidentiality of personally identifiable information;

- b. The terms and conditions of this MOA, including but not limited to the E2CCB Parents Bill of Rights for Data Security and Privacy and the Supplemental Information to Parents Bill or Rights for Data Privacy and Security, attached hereto as Exhibit A; and
- c. Applicable E2CCB policies, which can be accessed on the E2CCB website at: <https://go.boarddocs.com/ny/e2ccb/Board.nsf/Public>.

3. Contractor will use subcontractors in fulfilling its responsibilities to E2CCB, its employees or agents, and/or educational agencies which contract with E2CCB for the provision of Zoom's video communications services. Contractor manages its relationships with subcontractors to ensure the protection of personally identifiable information as set forth below.

Contractor has a vendor selection process that examines third-party risk. Contractor evaluates the SOC 2 reports for subcontractors as part of third-party risk management. Additionally, Contractor engages a third-party auditor to conduct a SOC 2 Type II audit of its subcontractors.

Contractor monitors SOC 2 reports and third-party security ratings of key vendors, subcontractors, and business partners involved in the processing and storing of customer data. As a public company, Contractor also monitors SOC 1 reports for certain third parties who are instrumental in the Contractor's service and financial reporting. Additionally, Contractor requires subcontractors who process personal data to enter into data processing agreements with comparable provisions related to confidentiality and data security, as well as employee and officer training.

Contractor agrees and acknowledges that the data protection obligations imposed on it by state and federal law, as well as the terms of this MOA shall apply to any subcontractor it engages in providing video communications services to E2CCB and any educational agencies that contract with E2CCB for the provision of Contractor's video communications services.

4. Contractor agrees that it will disclose student data and/or teacher or principal data only to those officers, employees, agents, subcontractors, and/or assignees who need access to provide the contracted services. Contractor further agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to that data.

Contractor has a formal documented Zoom Security Awareness and Training Policy, which defines Contractor's formal approach to security awareness and privacy training for all its employees. Furthermore, Contractor requires all employees to undergo security awareness and privacy training upon hire and yearly thereafter.

5. The exclusive purpose for which Contractor is being provided access to personally identifiable information is to provide the Services under the Master Agreement. Contractor does not monitor or use customer content for any reason other than as part of providing our services.

6. Student data and/or teacher or principal data received by Contractor, or by any subcontractor

or assignee of Contractor, shall not be sold or used for marketing purposes.

7. The agreement between Contractor and E2CCB for video communications services expires on June 30, 2020. Upon expiration of that agreement without a successor agreement in place, Contractor shall assist E2CCB and any educational agencies that contracts with E2CCB for the provision of Zoom's video communications services in exporting any and all student data and/or teacher or principal data previously received by Contractor back to E2CCB or the educational agency that generated the student data and/or principal data. Contractor shall thereafter securely delete or otherwise destroy any and all student data and/or teacher or principal data remaining in the possession of Contractor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data) as well as any and all student data and/or teacher or principal data maintained on behalf of Contractor in secure data center facilities. Contractor shall ensure that no copy, summary, or extract of the student data and/or teacher or principal data or any related work papers are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the extraction, transmission, deletion, or destruction of student data and/or teacher or principal data will be completed within 30 days of the expiration of the agreement between E2CCB and Contractor, and will be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. To the extent that Contractor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Contractor and/or its subcontractors or assignees will provide a certification to E2CCB from an appropriate officer that the requirements of this paragraph have been satisfied in full.

8. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by E2CCB or the educational agency that generated the student data for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the applicable educational agency's Annual Professional Performance Review Plan.

9. Student data and/or teacher or principal data transferred to Contractor will be stored in electronic format on systems maintained by Contractor in a secure data center facility located in the United States, or a data facility maintained by a Board of Cooperative Educational Services. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures shall include, but are not necessarily be limited to disk encryption, file encryption, firewalls, and password protection.

10. Contractor acknowledges that it has the following obligations with respect to any student data and/or teacher or principal data provided by E2CCB and/or the educational agencies which contract with E2CCB for the provision of Zoom's video communications services, and any failure

to fulfill one of these obligations set forth in New York State Education Law § 2-d and/or 8 N.Y.C.R.R. Part 121 shall also constitute a breach of its agreement with E2CCB:

- a. Limit internal access to education records to those individuals that are determined to have legitimate educational reasons within the meaning of § 2-d and the Family Educational Rights and Privacy Act;
- b. Not use education records/and or student data for any purpose other than those explicitly authorized in this Agreement;
- c. Not disclose any personally identifiable information to any other party who is not an authorized representative of Contractor using the information to carry out Contractor's obligations under this Agreement, unless (i) that other party has the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
- d. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody;
- e. 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);
- f. Notify E2CCB of any breach of security resulting in an unauthorized release of student data by Contractor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but not more than seven (7) calendar days after discovery of the breach;
- g. Where a breach or unauthorized release of personally identifiable information is attributable to Contractor, Contractor will pay or reimburse E2CCB and/or any educational agencies which contract with E2CCB for the provision of Zoom's video communications services for the cost of any notifications E2CCB and/or such other educational agencies is/are required to make by applicable law, rule, or regulation; and
- h. Contractor will cooperate with E2CCB and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.

11. In the event of a data security and privacy incident implicating the personally identifiable information of students, teachers, and/or principals of E2CCB or educational agencies which

contract with E2CCB for the provision of Contractor's video communications services:

- a. Contractor has an Incident Response Policy that is established to require the creation and maintenance of a structured Incident Response Plan to guide its response to security events, incidents, and breaches of the security of Contractor's services or corporate IT infrastructure.

Security incidents are reported and monitored by Security and Operations teams 24 hours per day, 7 days per week. All incidents are reported through Contractor's ticketing system. Contractor posts any general incident announcement and other announcements including scheduled maintenance, outages, and updates through our status page at status.zoom.us. Notification of 72 hours is provided when a data breach is confirmed.

- b. Contractor will notify E2CCB of any such incident in accordance with Education Law § 2-d, 8 N.Y.C.R.R. Part 121, and paragraph 10(f), above.

12. Any school district or BOCES within New York State may bind itself and Contractor to the terms of this MOA by opting into the terms of this MOA by informing E2CCB of its desire to do so in writing on a form prepared by E2CCB. Contractor's recourse in the event of a breach of this MOA by any school district or BOCES shall be limited to recourse against the breaching District or BOCES and shall not extend to any other District or BOCES.

13. This MOA, together with the signed Parents Bill of Rights for Data Privacy and the Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, constitutes the entire understanding of the Parties with respect to the subject matter thereof. The terms of this MOA, together with the signed Parents Bill of Rights for Data Privacy and the Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, shall supersede any conflicting provisions of Contractor's terms of service or privacy policy.

14. If any provision of this MOA shall be held to be invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable. If a court finds that any provision to this MOA is invalid or unenforceable, but that by limiting such provision it would become valid or enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.


15. This MOA shall be binding on any successors of the Parties.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

16. This MOA shall be governed by the laws of the State of New York. Any action or proceeding arising out of this contract shall be brought in the appropriate courts of New York State.

In witness of the foregoing, the duly authorized representatives of the Parties have signed this Memorandum on the date indicated.

FOR THE ERIE 2-CHAUTAUQUA-CATTARAUGUS BOCES:

DocuSigned by:

35052b4509E0400...


David O'Rourke, Ph.D
District Superintendent and Chief Executive Officer

Mar 31, 2020

Date

E2CC BOCES

FOR THE CONTRACTOR:

DocuSigned by:

12D13050014A4A7...

Kari Zeni
Associate General Counsel, Product & Compliance / DPO

Mar 31, 2020

Date

Zoom Video Communications, Inc.

EXHIBIT A: PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

E2CCB is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, E2CCB 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 to Parents Bill of Rights for Data Privacy and Security:

1. The exclusive purpose for which Contractor is being provided access to student data and/or teacher or principal data is to provide the Services under the Master Agreement. Zoom does not monitor or use customer content for any reason other than as part of providing our services.
2. Student data and/or teacher or principal data received by Contractor, or by any assignee of Contractor, will not be sold or used for marketing purposes.
3. Contractor agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data. More specifically, Contractor has a formal documented Zoom Security Awareness and Training Policy, which defines Contractor's formal approach to security awareness and privacy training for all its employees. Furthermore, Contractor requires all employees to undergo security awareness and privacy training upon hire and yearly thereafter. Contractor also requires subcontractors who process personal data to enter into data processing agreements with comparable provisions related to confidentiality and data security, as well as employee and officer training.

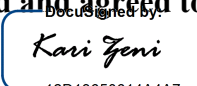
4. The agreement between Contractor and E2CCB for video communications services expires on June 30, 2020. Upon expiration of that agreement without a successor agreement in place, Contractor will assist E2CCB in exporting any and all student data and/or teacher or principal data previously received by Contractor back to E2CCB. Contractor will thereafter securely delete any and all student data and/or teacher or principal data remaining in its possession or the possession of its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data), as well as any and all student data and/or teacher or principal data maintained on its behalf of in secure data center facilities. Contractor will ensure that no copy, summary, or extract of the student data and/or teacher or principal data, or any related work papers, are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the extraction, transmission, deletion, or destruction of student data and/or teacher or principal data will be completed within thirty (30) days of the expiration of the agreement between BOCES and Contractor. To the extent that Contractor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they/it will not attempt to re-identify de-identified data and will not transfer de-identified data to any party.

5. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by the E2CCB for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the applicable educational agency's Annual Professional Performance Review Plan.

6. Student data and/or teacher or principal data transferred to Contractor will be stored in electronic format on systems maintained by Contractor in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

7. Any student data and/or teacher or principal data possessed by Contractor will be protected using encryption while in motion and at rest

Acknowledged and agreed to by:

Signature:  _____
Document signed by: Kari Zeni
12D13650614A4A7...

Name: Kari Zeni _____

Title: DPO _____

Date: Mar 31, 2020 _____

Zoom Video Communications, Inc.