

Completed Appendix C

**DATA SHARING AND CONFIDENTIALITY AGREEMENT
INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION**

1. Purpose

- a) This Appendix and Data Sharing and Confidentiality Agreement (“Agreement”) supplements any agreement between the parties and is intended to conform to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”). This Appendix consists of the terms of this Data Sharing and Confidentiality Agreement, and Exhibit A which is a copy of Onondaga-Cortland-Madison (OCM) BOCES’ Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information that is required to be posted on Onondaga-Cortland-Madison (OCM) BOCES’ website. Exhibit A is attached hereto and incorporated by reference.
- b) To the extent that any terms contained within the bidding documents, or any terms contained within any other written agreement between the parties, conflict with the terms of this Appendix, the terms of this Appendix will apply and be given effect. In the event that Vendor has online or written Terms of Service (“TOS”) that would otherwise be applicable to its customers or users of its Product that is the subject of these bidding documents to the extent that any term of the TOS conflicts, the terms of this Appendix will apply and be given effect.

2. Definitions

- 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 (as defined below) 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 Vendor by OCM BOCES, OCM BOCES officers, OCM BOCES employees, OCM BOCES agents, OCM BOCES students, and/or the officers, employees, agents, and/or students of educational agencies with whom OCM BOCES 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 Vendor by OCM BOCES, OCM BOCES officers, OCM BOCES employees, OCM BOCES agents, OCM BOCES students, and/or the officers, employees, agents, and/or students of educational agencies that contract with OCM BOCES in order to access Vendor’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.
- n) “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 these bid documents. For purposes of this Appendix, the term also includes BOCES or any other BOCES that is licensed to use Vendor’s Product pursuant to these bid documents to support its own educational programs or operations.

3. Confidentiality of Protected Data

- a) Vendor acknowledges that the Student Data and Teacher or Principal Data (collectively, “Protected Data”) it receives pursuant to these bid documents 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) and any applicable BOCES’ policy on data security and privacy. Vendor acknowledges BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, but that adoption may not occur until a date subsequent to the effective date of an award to a successful bidder under these bid documents. BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption, and Vendor and BOCES agree to engage in good faith negotiations to modify this Agreement to the extent necessary to ensure Vendor’s continued compliance with Section 2-d.
- c) Protected Data received by Vendor shall not be sold or used for marketing purposes.

- d) The exclusive purpose for which Vendor is being provided access to Personally Identifiable Information is to provide the **software and associated deployment and support services detailed in this RFB**. Vendor does not monitor or use customer content for any reason other than as part of providing our services.

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 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 Agreement, consistent with BOCES' data security and privacy policy, Vendor's shall perform as follows:

All Bidder software and related services are governed by an "evergreen" Information Security Policy (ISP) informed by routine risk analysis, industry best practices, and legal standards for the housing and management of legally protected information (PI). The Bidder's ISP meets the criteria for compliance required for "Business Associates" under the HIPAA Security and HIPAA Privacy Rules and legislation governing the appropriate storage and handling of student and teacher personally identifiable information (PII) by "3rd-Party Contractors," including (but not limited to) NYS Education Law 2-d.

The Bidder will implement and maintain all state, federal and local data security and privacy requirements over the term of the Agreement in a manner that is consistent with the data security and privacy policies of the OCM BOCES and each Participating Educational Agency that purchase Bidder's products and/or services pursuant to the Agreement by maintaining the implementation of required administrative, physical, and technical safeguards stipulated in the regulations.

The Administrative Safeguard Standard, "Evaluation," requires the periodic technical and nontechnical evaluation of the Bidder's compliance in response to environmental and/or operational changes affecting the security of Customer data. Changes to state, federal and local data security and privacy requirements are defined as in-scope "environmental changes" and, as such, are monitored, evaluated, and integrated (or otherwise appropriately responded to) with other environmental and operational changes impacting the security and privacy of protected data to ensure consistent Bidder compliance.

When a new Participating Educational Agency becomes a user of Bidder software and associated deployment and support services pursuant to this RFB, the Bidder will review and sign the Agency's "Parent's Bill of Rights" and supplemental data security and privacy-related provisions, provided such requirements do not conflict with or weaken the Bidder's implemented administrative, physical, and technical safeguards and practices or violate applicable laws and regulations.

- b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the agreement between the parties:

Administrative/Operational Safeguards:

- **Security Management Process – Risk analysis procedure, risk management procedure, sanction policy, information system activity monitoring and review procedures.**

- Assigned Data Privacy and Security Responsibility – “Information Security Officer” responsible for the administration of SchoolFront information privacy and security policies and procedures.
- Workforce Security – Authorization and/or supervision definition, workforce clearance procedure, termination procedures, workforce development procedure.
- Information Access Management - Isolation of data and functions in systems using least privileged model of authentication, access authorization procedures, access establishment and modification guidelines and procedures.
- Security Awareness and Training – Training and routine security and privacy-related communication/reminders, content explicitly addressing protection from malicious software and external threats, content addressing SchoolFront requirements under applicable laws and regulations, content explicitly explaining SchoolFront policies and procedures developed to protect Customer data, monitoring of all system/data access and usage, password management/policy.
- Security Incident Procedures – Response and Reporting
- Contingency Plan – Data backup policy, disaster recovery procedure, emergency operation plan, testing and revision procedure, applications/data criticality analysis.
- Routine Evaluation – Periodic technical and nontechnical evaluation of SchoolFront’s implemented administrative, physical, technical safeguards, and practices.
- Policies and Procedures for Third-Party Relationships – Only applicable if such relationships are allowed by the Agreement.

Physical Safeguards:

- Facility Access Controls - Contingency operations, facility security plan, access control and validation procedures, maintenance records
- Workstation Use - Acceptable Use Policies for Assets and Data, Context-, Device-, and Location-specific Policies and Procedures for the secure access of systems and data.
- Workstation Security - Secure workstations, hardware, and devices to restrict access to authorized users.
- Device and Media Controls – Disposal, media re-use, accountability, data backup and storage

Technical Safeguards:

- System/Data Access Control - Unique user identification, emergency access procedure, automatic logoff, encryption and decryption.

- Audit Controls – Hardware/software/procedural mechanism(s) to log and analyze activity in SchoolFront information systems that house or use Customer data.
- Integrity – Mechanism(s) to protect Customer data from improper alteration or destruction.
- Person or Entity Authentication – Mechanism(s) to validate the identities of persons/entities accessing SchoolFront systems and prevent unvalidated access.
- Transmission Security – Integrity controls, encryption.

- c) Vendor will comply with all obligations set forth in BOCES’ “Supplemental Information” as set forth 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:

Bidder officers and employees who will have access to protected data will receive routine training on the federal and state laws governing the confidentiality of such data prior to receiving access to the data. Bidder employee training is provided by Global Compliance Network (GCN) Training (or an equally qualified training vendor) during the new officer/employee (or new position) “onboarding” period with “refresher” training delivered annually (or when major changes to legislation occur) thereafter.

- e) Vendor [check one] _____ will will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under these bid documents. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under these bid documents, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in BOCES’ “Supplemental Information” below.
- f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section ____ 5 below.
- g) Upon expiration or termination of any agreement between the parties without a successor agreement in place, Vendor shall assist OCM BOCES and any Participating Educational Agency for the provision of Vendor’s services in exporting any and all Protected Data previously received by Vendor back to OCM BOCES or the Participating Educational Agency that generated the Protected Data. Vendor shall thereafter securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor 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 Protected Data maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary, or extract of the Protected Data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the extraction, transmission, deletion, or destruction of Protected Data will be completed within 30 days of the expiration/termination of the agreement between OCM BOCES and Vendor, 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 Vendor 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,

Vendor and/or its subcontractors or assignees will provide a certification to OCM BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

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 considered a breach including a breach of the terms of this Agreement:

- a) Limit internal access to Protected 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).
- 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 these bid documents.
- c) Not use Protected Data for any purposes other than those explicitly authorized in this Agreement.
- 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, 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 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);
- g) Provide notification to Onondaga-Cortland-Madison (OCM) BOCES (and Participating Educational Agencies), of any breach of security resulting in an unauthorized release of Protected Data 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
- h) Where a breach or unauthorized release of Protected Data is attributable to Vendor, Vendor will pay or reimburse OCM BOCES and/or any Participating Educational Agencies for the full cost of any notifications OCM BOCES and/or such other Participating Educational Agencies is/are required to make by applicable law, rule, or regulation; and
 - i. Vendor will cooperate with OCM BOCES, any Participating Educational Agency, and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

6. Notification of Breach and Unauthorized Release

In the event of a data security and privacy incident implicating the Protected Data of OCM BOCES or Participating Educational Agencies:

- a) Vendor shall:

Initiate our breach mitigation procedures which include notifying OCM BOCES, and any Participating Agency, of any such incident in accordance with Education Law § 2-d, 8 N.Y.C.R.R. Part 121.

- b) Vendor will notify OCM BOCES, and any Participating Agency, of any such incident in accordance with Education Law § 2-d, 8 N.Y.C.R.R. Part 121, and the provisions contained herein and 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.
- c) Vendor will cooperate with Onondaga-Cortland-Madison (OCM) BOCES and Participating Agency and provide as much information as possible directly about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.
- d) Vendor acknowledges that upon initial notification from Vendor, Onondaga-Cortland-Madison (OCM) 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 Onondaga-Cortland-Madison (OCM) BOCES, Vendor will promptly inform OCM BOCES in writing.
- e) Vendor will consult directly with OCM BOCES 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.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

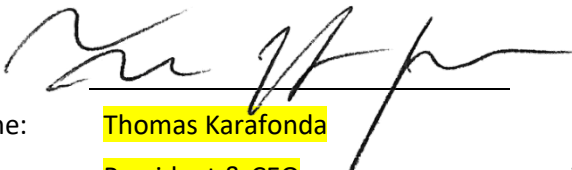
7. Miscellaneous

- a) The terms of this Agreement, 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 Vendor's terms of service or privacy policy.
- b) If any provision of this Agreement 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 Agreement 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.
- c) This Agreement shall be governed by the laws of the State of New York. The Parties hereto agree that exclusive venue for any litigation, action or proceeding arising from or relating to this Agreement shall lie in the state and federal courts located in Onondaga County, New York, and the Parties expressly waive any right to contest such venue for any reason whatsoever.

In witness of the foregoing, the duly authorized representatives of the Parties have executed this Agreement as of the date both parties have signed below.

VENDOR

OCM BOCES

By: 
Name: **Thomas Karafonda**
Title: **President & CEO**
Date: **4/2/2024**

By: _____
Name: _____
Title: _____
Date: _____

OCM BOCES PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

This Exhibit A is part and parcel to the Data Privacy and Security Agreement dated **4/2/2024** by and between Vendor and the Onondaga Cortland Madison Board of Cooperative Educational Services (“OCM BOCES”).

OCM BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, OCM BOCES wishes to inform the community of the following:

1. A student’s Personally Identifiable Information (PII) cannot be sold or released for any commercial or marketing purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. This right of inspection is consistent with the requirements of the Family Educational Rights and Privacy Act (FERPA). In addition to the right of inspection of the educational record, Education Law §2-d provides a specific right for parents to inspect or receive copies of any data in the student’s educational record.
3. State and federal laws protect the confidentiality of PII, 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 parents may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
5. Parents have the right to file complaints with OCM BOCES/CNYRIC about possible privacy breaches of student data by OCM BOCES/CNYRICs third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints regarding student data breaches should be directed to: Chantal M. Corbin, Director, OCM BOCES/CNYRIC, 6075 East Molloy Road, PO Box 4866, Syracuse, NY 13221. Phone: 315-433-8300; e-mail: ccorbin@cnyric.org.
6. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email: CPO@mail.nysed.gov.


Supplemental Information to Parents Bill or Rights for Data Privacy and Security:

1. The exclusive purpose for which Vendor is being provided access to student data and/or teacher or principal data is to the **facilitate the use of the SchoolFront Employee Management System and Document Repository**. Vendor 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 Vendor or by any assignee of Vendor, will not be sold or used for marketing purposes.
3. Vendor agrees that any of its officers or employees 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, Vendor **has given its officers or employees who have access to personally identifiable information compliant training by Global Compliance Network (GCN) Training and will continue to provide training (facilitated by GCN or an equally qualified training vendor) for new officers, employees, or employees who change roles in the organization entailing new access to protected data.**

Furthermore, Vendor requires all employees to undergo security awareness and privacy training upon hire and yearly thereafter.

4. Upon expiration or termination of the agreement between the parties, without a successor agreement in place, Vendor will assist OCM BOCES and any Participating Educational Agency in exporting any and all student data and/or teacher or principal data previously received by Vendor back to OCM BOCES. Vendor will thereafter securely delete any and all student data and/or teacher or principal data remaining in its possession (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. Vendor 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 Vendor 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 Vendor. To the extent that Vendor 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 OCM BOCES 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 Vendor will be stored in electronic format on systems maintained by Vendor 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, Vendor 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 Vendor will be protected using encryption technology while in motion, in its custody and at rest.

Acknowledged and agreed to by:

Signature: 

Name: Thomas Karafonda

Title: President & CEO

Date: 4/2/2024