DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Cheektowaga-Sloan UFSD Bill of Rights for Data Security and Privacy
and
Supplemental Information about a Master Agreement between
Cheektowaga-Sloan UFSD and **[Notable Inc (dba Kami)]**
In the event of a contradiction between this agreement and any other agreement, this agreement will apply.

1. **Purpose**

(a) Pursuant to New York State Education Law 2-d, educational agencies that enter into contractual arrangements with third-party contractors must take additional steps to secure certain personally identifiable information that may be transmitted between the parties. These steps include but are not limited to enacting and complying with a Parents "Bill of Rights" relative to protected data; ensuring that each third-party contractors has a detailed data privacy plan in place to ensure the security of such data; and that certain third-party vendors provide a signed copy of the educational agency's Bill of Rights, thereby signifying that the vendor will comply with such Bill of Rights. The Master Services Agreement, Exhibits, and Statement of Work(s) are subject to the requirements of Education Law 2-d.

(b). The District considers Provider as a third-party contractor, and as such, the parties must comply with the requirements under New York Education Law 2-d. The Services described under the applicable Statement of Work(s) indicate that Provider may receive student, teacher or principal data "Personally Identifiable Information") and other non-public information, which includes, but is not limited to, student, teacher and principal data, metadata, and user content (collectively referred to as" Protected Data.") that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). Such Protected Data, which includes, Personally Identifiable Information, may be shared with Provider to assist Provider with the completion of services or deliverables.

(c) This Exhibit is intended to supplement the terms and conditions located in the Master Agreement and sets forth the requirements of Section 2-d that must be adhered to by both parties throughout the Term of the Agreements. Exhibit A consists of a Data Sharing and Confidentiality Agreement, a copy of the Client's Bill of Rights for Data Security and Privacy signed by Provider, and supplemental information about the Master Agreement between Cheektowaga-Sloan UFSD and [Name of Provider] that the Client is required by Section 2-d to post on its website.

(d) In the event of a conflict between the terms contained in the Master Service Agreement, Exhibit A, Statement of Work(s) or any other written terms between the Parties, the order of precedence will be as follows: (1) Exhibit A; (2) Master Service Agreement; and (3) Statement of Work(s); unless the Parties specifically reference the provision contained in the MSA or Exhibit A that it intends to supersede. Client will not be bound by any terms and conditions contained in Provider's online Terms of Service, License Agreement, or Purchase Order terms and conditions.

2. Definitions

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Provider may receive from the Client pursuant to the Master Agreement.

(b) "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Provider may receive from the Client pursuant to the Master Agreement.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service being provided to the Client by Provider pursuant to the Agreements and other non-public information, which includes, but is not limited to, student, teacher and principal data, metadata, and user content.

(d) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. Confidentiality of Protected Data

(a) Provider acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the Client or Client End User and that such Protected Data belongs to and is owned by the Client.

(b) Provider will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law, including but not limited to New York Education Law Section 2-d and the Client's policy on data security and privacy. Provider will treat "Protected Data" as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as Provider uses to protect its confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Services Agreement and applicable Statement of Work(s), Provider will have and maintain a Data Security and Privacy Plan (the "Plan") in place to protect the confidentiality, privacy, and security of the Protected Data it receives from the Client, students, teachers, principals or administrators.

Provider's Plan for protecting the Client's Protected Data includes, but is not limited to, its Agreement to comply with the terms of the Client's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Provider.

The Provider's Data Security and Privacy Plan must also contain the following additional components:

(a) The Plan will comply with all state, federal, and local data security and privacy requirements, including but not limited to: the Children's Internet Protection Act; Family Educational Rights and Privacy Act; Health Insurance Portability and Accountability Act of 1996, if applicable; the terms contained in the MSA, SOW(s), this Exhibit A; and any other terms and conditions agreed upon between the parties that pertain to data security and privacy.

(b) Prohibits the use of any Data received by the Client to market or advertise to students, teachers, or parents.

(c) Providers will have specific administrative, operational, and technical safeguards and practices in place to protect Protected Data that it receives under the Agreements.

(d) Provider must execute written agreements with any subcontractors or any other authorized persons or entities to whom it may disclose Protected Data (if any) that contain requirements to comply with all federal, state and local laws applicable to the types of services performed and requires them to adhere to all the provisions set forth in the Agreements, including but not limited to the procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent permitted) as outlined in the Agreements.

(e) Provider has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, before their receiving access.

(f) Provider will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Provider will provide prompt notification to the Client of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Exhibit.

5. Notification of Breach and Unauthorized Release

(a) Provider will promptly notify the Client of any breach or unauthorized release of Protected Data collected under the Agreements in the most expedient way possible and without unreasonable delay. Still, no more than seven (7) calendar days after Provider has discovered or been informed of the breach or unauthorized release.

(b) Provider will provide such notification to the Client by contacting Brian Zybala directly by email at bzybala@cheektowagasloan.org or by calling 716-897-7800 ext 2125.

(c) Provider will cooperate with the Client and provide as much information as possible directly to Brian Zybala or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Provider discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the Client affected, what the Provider 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 Provider representatives who can assist affected individuals that may have additional questions.

(d) Provider acknowledges that upon initial notification from Provider, the Client, as the educational agency with which Provider contracts, has an obligation under Section 2-d to, in turn, notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Provider agrees not to provide this notification to the CPO directly unless requested by the Client or otherwise required by law. In the event the CPO contacts Provider directly or requests more information from Provider regarding the incident after having been initially informed of the incident by the Client, the Provider will promptly inform Brian Zybala or his/her designee.

6. Data Processing and Transfers. With respect to any Processing of Protected Data, which includes Personally Identifiable Information, Provider (i) has full legal authority in each jurisdiction where Protected Data will be Processed to Process such Protected Data; (ii) will Process such Protected Data only on behalf of the Client as necessary to carry out its obligations under the Agreement and only in accordance with the instructions of Client; (iii) will not Process

such Protected Data for purposes incompatible with those for which it was collected or subsequently authorized by the data subject; and (iv) has complied, and will comply, with all applicable Privacy Laws. Provider can maintain or use de-identified data received by Client, but Provider will not be permitted to re-identify the data and will restrict any party receiving such data from re-identifying the data.

7. Data Return or Destruction. Promptly upon the expiration or earlier termination of any Statement of Work, or such earlier time as Client requests, Provider shall, and shall cause approved subcontractors or third-party providers to, return to Client, or at Client's request, destroy or render unreadable or undecipherable if return is not reasonably feasible or desirable to Client (which decision shall be based solely on Client's written statement), each and every original and copy in every media of all Protected Data in the possession, custody or control of Provider and its approved subcontractors or third-party providers. Promptly following any return or alternate action taken to comply with this subsection. In the event applicable law does not permit Provider or any Provider Representative to comply with the delivery or destruction of the Personally Identifiable Information, Provider warrants, and shall cause any such Provider Representative to warrant, that it shall ensure the confidentiality of the Personally Identifiable Information and that it shall not Process any Personally Identifiable Information disclosed by or on behalf of Client after termination of the applicable Statement of Work.

8. **Additional Statutory and Regulatory Obligations** Provider acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received under the Agreements, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a material breach of the Agreements:

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

(b) Limit internal access to Protected Data to those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA) and need access in order to assist Provider in fulfilling one or more of its obligations to the Client under the Agreements.

(c) To not use education records or Protected Data for any purposes other than those explicitly authorized under the Agreements.

(d) To not disclose any Protected Data to any other party, except for authorized representatives of Provider using the information to carry out Provider's obligations to the Client and in compliance with state and federal law, regulations and the terms of the Master 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 Client no later than the time of disclosure, unless such notification is expressly prohibited by the statute or court order.

(e) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(f) To use encryption technology to protect Protected Data in its custody while in motion or at rest,
using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(g) Where the student, 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 such data will be encrypted.

(h) To adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework.

(i) To comply with the Client's policy on data security and privacy, Section 2-d and Part 121.

(j) To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(k) To notify the Client, in accordance with the provisions of Section 5 of this Exhibit, of any breach of security resulting in an unauthorized release of Protected Data by Provider or its assignees or subcontractors in violation of applicable state or federal law, the Client's Bill of Rights for Data Security and Privacy, the Client's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Agreements.

(l) To cooperate with the Client and law enforcement to protect the integrity of investigations into
the breach or unauthorized release of Protected Data.

(m) To pay for or promptly reimburse the Client for the full cost of notification, in the event the Client is required under Section 2-d to notify affected parents, students, teachers, or principals of a breach or unauthorized release of Protected Data attributed to Provider or its subcontractors or assignees.

Bill of Rights for Data Security and Privacy

Cheektowaga-Sloan Union Free School District

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Cheektowaga-Sloan Union Free School Client is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the Client informs the school 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 records.
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 New York State is available for public review at the following website http://www.nysed.gov/student-data-privacy/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 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 Privacy Complaint, 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/student-data-privacy/form/report-improper-disclosure.

BY THE PROVIDER:

Bob Drummond

Name (Print)

Signature

Data Protection Officer

Title

9/22/2020

Date