DATA PRIVACY AND SECURITY TERMS AND CONDITIONS

for the Master Agreement between
Hamburg Central School ("District") and [Name of Vendor] ("Vendor")
(collectively the "Parties")

WHEREAS, the District and Vendor are parties to a contract or other written agreement for purposes of providing certain products or services to the District ("Master Agreement"); and

WHEREAS, Education Law §2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") require the Parties to have certain terms and conditions governing the privacy and security of certain data the Vendor will receive pursuant to the Master Agreement; and

WHEREAS, the Parties are desirous to set forth such terms and conditions in this Exhibit to the Master Agreement;

NOW THEREFORE, in consideration of the mutual promises set forth in the Master Agreement, the Parties agree to the following terms and conditions.

A. DEFINITIONS

1. "Student Data" means personally identifiable information from the student records of the District that Vendor receives pursuant to the Master Agreement.

2. "Teacher or Principal Data" means personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under Education Law §§ 3012-c and 3012-d that Vendor receives pursuant to the Master Agreement.

3. "Protected Data" means Student Data and/or Teacher or Principal Data, as defined above.

B. PURPOSE

1. Pursuant to the Master Agreement, the Vendor will receive Protected Data from the District for purposes of providing certain products or services to the District.

2. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with these Terms and Conditions , these Terms and Conditions will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, these Terms and Conditions shall supersede any conflicting terms of the TOS.

C. DATA SHARING AND CONFIDENTIALITY

1. Vendor Acknowledgments

i. Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

ii. 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 will comply with the District's policy on data privacy and security. The District will provide Vendor with a copy of its policy on data privacy and security upon request.

2. Vendor's Data Privacy and Security Plan

i. Vendor will implement all state, federal, and local data privacy and security requirements and such requirements contained within the Master Agreement and these Terms and Conditions including but not limited to the requirements set forth in the Parents' Bill of Rights and the Supplemental Information set forth below, consistent with the District's data privacy and security policy.

ii. Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

iii. Vendor 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 assignees, if applicable, who will have access to Protected Data, prior to receiving access.

iv. If Vendor uses any subcontractor(s), Vendor will require such subcontractor(s) or other authorized persons or entities to whom it may disclose Protected Data to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law, the Master Agreement, and these Terms and Conditions shall apply to the subcontractor.

v. Vendor will follow certain procedures for the return, transition, deletion, and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement as set forth in detail in the Supplemental Information below.

vi. Vendor will manage data privacy and security incidents that implicate Protected Data and will develop and implement plans to identify breaches or unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 3 herein.

3. Notification of Breach or Unauthorized Release

With respect to any breach or unauthorized release of Protected Data, including any breach or unauthorized release of Protected Data by Vendor's assignees or subcontractors, Vendor acknowledges and agrees to the following:

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

ii. Vendor will provide such notification to the District by contacting Data Privacy Officer directly by email at dataprotection@hcsdk12.org or by calling 716-646-3280 ext. 4136.

iii. Vendor will cooperate with the District and provide as much information as possible directly to Data Privacy Officer or his/her designee 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 Protected Data involved, an estimate of the number of records affected, the schools within the District 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.

iv. Vendor acknowledges that upon initial notification from Vendor, the District has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide such notification to the CPO directly unless requested by the District or otherwise required by law. 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 the District, Vendor will promptly inform Data Privacy Officer or his/her designee.

v. Vendor will cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

vi. Vendor will pay for or promptly reimburse the District for the full cost of notification, in the event the District 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 Vendor, its subcontractors or assignees.

4. Additional Statutory and Regulatory Obligations

Vendor acknowledges additional obligations under Section 2-d and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach

of the Master Agreement and these Terms and Conditions. Vendor acknowledges and agrees to the following:

i. To limit internal access to Protected Data to only those employees or subcontractors that need access to the Protected Data in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

ii. To not use Protected Data for any purposes not explicitly authorized in the Master Agreement or these Terms and Conditions.

iii. To not disclose any Protected Data to any other party, except for authorized employees, subcontractors, or assignees of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

a. the parent or eligible student provided prior written consent; or

b. the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

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

v. To use encryption to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified or permitted 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.

vi. To adopt technologies, safeguards and practices that align with the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, "NIST Cybersecurity Framework" (Version 1.1).

vii. 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.

D. PARENTS' BILL OF RIGHTS AND SUPPLEMENTAL INFORMATION

1. Parents' Bill of Rights

Vendor acknowledges and agrees that the District's Parents' Bill of Rights as set forth herein and as posted on the District's website is incorporated into these Terms and Conditions.

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Hamburg Central School District 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 District 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 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 New York State is available for public review at the following website http://www.nysed.gov/data-privacy-security/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/data-privacy-security/report-improper-disclosure.

Supplemental Information Regarding Third-Party Contractors

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

Each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District will include the following information:

1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);

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;

5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and

6) Address how the data will be protected using encryption while in motion and at rest.

2. Supplemental Information

i. The exclusive purpose for which Protected Data will be used is [*Describe Specific Products/Services Provided by Vendor*]. Vendor will not use the Protected Data for any other purposes not explicitly authorized herein or within the Master Agreement.

ii. In the event that Vendor engages subcontractors or other authorized persons or entities ("Subcontractors") to perform one or more of its obligations under the Master Agreement (including hosting of the Protected Data), Vendor will require Subcontractors to execute legally binding agreements acknowledging and agreeing to comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement, these Terms and Conditions, and applicable state and federal law and regulations.

iii. The Master Agreement commences on [Date] and expires on [Date]. Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will (select all that apply):

☐ Securely delete or otherwise destroy all Protected Data remaining in the possession of Vendor or any of its Subcontractors.

☐ Assist the District in exporting and returning all Protected Data previously received to the District in such formats as may be requested by the District.

☐ Contact the District requesting instruction for the deletion or return of all Protected Data.

In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.

Neither Vendor nor any Subcontractors will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or Subcontractors will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

iv. Parents or eligible students can challenge the accuracy of any Protected Data in accordance with the District's procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

v. Any Protected Data will be stored on systems maintained by Vendor, or Subcontractor(s) under the direct control of Vendor, in a secure data center facility. The measures that Vendor (and, if applicable, Subcontractor(s)) will take

to protect Protected Data include adoption of technologies, safeguards and practices that align with the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, "NIST Cybersecurity Framework" (Version 1.1) and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

vi. Vendor (and, if applicable, Subcontractor(s)) will use encryption to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified or permitted 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.

3. Posting

In accordance with Section 2-d, the District will publish the Parents' Bill of Rights and Supplemental Information from these Terms and Conditions on its website. The District may redact the Parents' Bill of Rights and Supplemental Information to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

IN WITNESS WHEREOF, the Parties have indicated their acceptance of these Terms and Conditions including the Parents' Bill of Rights and Supplemental Information by their signatures below on the dates indicated.

BY THE VENDOR:

_____
Name (Print)

_____
Signature

_____
Title

_____
Date

BY THE DISTRICT:

_____
Name (Print)

_____
Signature

_____
Title

_____
Date