EXHIBIT A

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

AND

SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. Purpose

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms 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 Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of BOCES Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on BOCES website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit 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 the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. Definitions

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "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 the MLSA. For purposes of this Exhibit, the term also includes BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. Confidentiality of Protected Data

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA 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 BOCES policy on data security and privacy. Vendor acknowledges that 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 the MLSA. 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 Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

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 Data Sharing and Confidentiality Agreement, consistent with BOCES data security and privacy policy, Vendor will:

[*Please see attached KMS Privacy Policy and Security Plan Documents.]

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

[*Please see attached KMS Privacy Policy and Security Plan Documents]

c. Vendor will comply with all obligations set forth in BOCES "Supplemental Information about the MLSA" 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:

[*Please see attached KMS Privacy Policy and Security Plan Documents. Additionally, all staff are trained upon hire and we conduct annual compliance trainings with all employees.]

e. Vendor [check one] ___will **__X_will not** utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in BOCES "Supplemental Information about the MLSA," 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 of this Data Sharing and Confidentiality Agreement.

g. Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in BOCES "Supplemental Information about the MLSA," below.

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 a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records 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).
   (i) 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 the MLSA.
   (ii) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(b) 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 under the MLSA, unless:

(c) the parent or eligible student has provided prior written consent; or

(d) 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 that complies with Section 2-d, as more fully set forth in BOCES "Supplemental Information about the MLSA," below.

(g) Provide notification to BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of

any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are 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 or its subcontractors or assignees.

6. Notification of Breach and Unauthorized Release

(a) Vendor shall promptly notify BOCES 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.

(b) Vendor will provide such notification to BOCES by contacting Michele Jones directly by email at Michele.jones@neric.org or by calling (518) 464-5139 (office).

(c) Vendor will cooperate with BOCES and provide as much information as possible directly to the General Counsel or 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 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, 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 BOCES, Vendor will promptly inform General Counsel or designees.

(e) Vendor will consult directly with General Counsel or designees 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.

EXHIBIT A (CONTINUED)

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Albany-Schoharie-Schenectady-Saratoga BOCES (BOCES) is committed to protecting the privacy and security of personally identifiable information about students who attend BOCES instructional programs in accordance with applicable law, including New York State Education Law Section 2-d.

To further these goals, BOCES wishes to inform parents 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 may be directed to the NYS Chief Privacy Officer by writing to the 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.

BY THE VENDOR: Kinney Management Services LLC

Name: Sandra Steinhardt

Signature: Sandra Steinhardt

Title: Managing Member

Date: 3-23-2023

EXHIBIT A (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT

BETWEEN

Albany-Schoharie-Schenectady-Saratoga BOCES AND Kinney Management Services LLC

BOCES has entered into a Master License and Service Agreement ("MLSA") with Kinney Management Services LLC ("Vendor"), which governs the availability to Participating Educational Agencies of the following Product(s):

Ksystems and Kchecks

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used:

To assist the District with meeting various documentation and reporting requirements for securing Medicaid funding for School Supported Health Related Services (SSHSP) provided to students.

To be completed by Vendor:

The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors:

In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: [Describe steps the Vendor will take]

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on 7/1/2023 and expires on 6/30/2024. Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors. If requested by a Participating Educational Agency, Vendor will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion.

• At BOCES request, Vendor will cooperate with BOCES as necessary in order to transition Protected Data to any successor Vendor(s) prior to deletion.

• Vendor agrees that neither it nor its subcontractors, assignees, or other authorized agents will retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors, assignees, or other authorized agents will provide a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data:

Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections:

Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data:

Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

Data Privacy and Security Policy v3.21

Kinney Management Services LLC -- Kinney Services, Inc.
1205 Troy Schenectady Road Suite 106 Latham New York 12110 (518) 371-0176

1. Purpose

This policy addresses Kinney Management Services LLC and Kinney Services Inc. responsibility to adopt appropriate administrative and technical safeguards to protect personally identifiable information (PII) collected by our staff and our systems. The electronic restrictions and safeguards outlined in this policy provide guidance for our employees that have access to PII to ensure compliance with state and federal regulations.

2. Scope

This policy applies to all Kinney employees, interns, consultants and third parties who receive or have access to data stored on one of Kinney's systems (Users). This policy encompasses all systems, automated and manual, and all information regardless of the form or format which is created or used in support of the activities of Kinney on behalf of our clients.

3. Policy Statement

It is the responsibility of Kinney:

A. to comply with legal and regulatory requirements governing the collections, retention, dissemination, protection and destruction of information;
B. to maintain a comprehensive Data Privacy and Security program designed to satisfy these regulatory obligations;
C. to protect personally identifiable information and sensitive and confidential information from unauthorized use or disclosure;
D. to provide annual compliance training to its employees on federal and state laws and regulations regarding the protection of PII;
E. to provide training to its employees on online privacy and security measures;
F. to communicate its required data security and privacy responsibilities to all systems users.

4. Standard

Kinney will utilize the National Institute of Standards and Technology's Cybersecurity Framework v1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program.

5. Data Privacy

1. Laws such as FERPA, NYS Education Law 2-d Part 121 and other state or federal laws establish baseline parameters for what is permissible when sharing PII.
2. Data protected by law must only be used in accordance with law and regulation to ensure it is protected from unauthorized use and/or disclosure.
3. No Student data or any other PII shall be shared with third parties without written agreement that complies with State and federal laws and regulations. No student data or other PII will be provided to third parties unless it is required by a court of law.

6. Definitions

A. Personally Identifiable Information (PII) – is any information pertaining to an individual that can be used to distinguish or trace a person's identity. Some information that is considered PII is available in public sources such as telephone books, public websites, etc. This type of information is considered to be *Public* PII and includes:

1. First and Last name
2. Address
3. Work telephone number
4. Work e-mail address
5. Home telephone number
6. General educational credentials
7. Photos and video

In contrast, *Protected* PII is defined as any one or more of types of information including, but not limited to:

1. Social security number
2. Username and password
3. Passport number
4. Credit card number
5. Clearances
6. Banking information
7. Date and place of birth
9. Mother's maiden name
10. Criminal, medical and educational records

If a question arises about what is or isn't PII please contact our Information Security Department at kmsis@kinneyassoc.com.

7. Procedures

A. General

This section provides guidelines on how to maintain and discard PII. If current procedures fall outside this policy or questions arise please contact Sandy Steinhardt at skinney@kinneyassoc.com. All electronic files that contain Protected PII will reside within a protected information system location. All physical files that contain Protected PII will reside within a locked file cabinet or room when not being actively viewed or modified. Protected PII is not to be downloaded to personal workstations or mobile devices (such as laptops, mobile phones, tablets or removable media) or to systems outside the protection of the Kinney network. PII will also not be sent through any form of insecure electronic communication E.g. E-mail or instant messaging systems. Significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII the physical or electronic file should be shredded or securely deleted. For help with secure deletion please contact our Information Security Department at kmsis@kinneyassoc.com .

B. Incident Reporting

The Information Security Department must be informed of a real or suspected disclosure of Protected PII data within 12 hours after discovery. E.g. Misplacing a paper report, loss of a laptop, mobile device, or removable media containing PII, accidental email of PII, possible virus, or malware infection or a computer containing PII.

C. Enforcement

An employee found to be in violation of this policy may be subject to disciplinary action as deemed appropriate based on the facts and circumstances giving rise to the violation.

Network Security Summary

This report summarizes the /Kinney Management Services LLC - Kinney Services, Inc. network physical security controls, hardware systems monitoring, firewall protection, antivirus, and data retention systems.

Network Management

Kinney Services utilizes 24/7 network monitoring and management. This system generates daily hardware reports as well as immediately informing us when set parameters have triggered an alarm.

Network Firewall

Kinney Services employs an industry standard firewall to protect our network against internet threats. Kinney services only allows connections from the United States into our network. The firewall records all connections and forwards them to a syslog server. An internal program permanently imports these entries into our SQL database. The log summaries are reviewed daily for any abnormalities and blocks are put into place when suspicious activity is detected.

Workstation and Server Virus Protection

Kinney Services utilizes antivirus on the firewall monitoring traffic (updated every 4 hours) and antivirus on our networked systems (also updated every 4 hours). We also employ Microsoft Office 365 to provide phishing, antivirus and spam protection.

Data Protection

All data is backed up locally on our large array and remotely on Microsoft Azure Secure Storage. All data backed up to Microsoft Azure is pre-encrypted during the local backup before it leaves our server as well as encrypted at rest on Microsoft Azure.

External and Internal Network Security Scans

External and internal network security scans are done at regular intervals.

Physical Security

We are in a building with a keypad-controlled entrance after regular business hours, a full-time keypad-controlled entrance for the Kinney Services office and a full-time keypad-controlled entrance for the server room (within the office). An alarm system with cameras, temperature sensors and remote monitoring is also installed within our office. We have additional temperature monitoring for the environmental systems in our server room. Our power systems are backed up by multiple UPS systems as well as a natural gas generator.

If you have further questions or concerns, please contact:

John Janes, Director of IT | Phone (518) 371-0176 | jajanes@kinneyassoc.com

Sandy Kinney Steinhardt, President/Managing Member | Phone (518) 371-0176 | skinney@kinneyassoc.com

1205 Troy Schenectady Road Suite 106 Latham, NY 12110