EXHIBIT A

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE
Agreement

1. **Purpose**

(a) This Exhibit supplements the KIDS DISCOVER, LLC ("AGREEMENT") to which it is attached, to ensure that the AGREEMENT 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 KIDS DISCOVER, LLC, and the Supplemental Information about the Agreement that is required to be posted on BOCES website.

(b) To the extent that any terms contained within the AGREEMENT, or any terms contained within any other Exhibits attached to and made a part of the AGREEMENT, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that KIDS DISCOVER 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 AGREEMENT, 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 AGREEMENT will have the same definition as contained within the AGREEMENT.

In addition, as used in this Exhibit:

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

(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 KIDS DISCOVER receives from a Participating Educational Agency pursuant to the AGREEMENT.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to KIDS DISCOVER'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 KIDS DISCOVER's Product pursuant to the terms of the AGREEMENT.

3. **Confidentiality of Protected Data**

(a) KIDS DISCOVER acknowledges that the Protected Data it receives pursuant to the AGREEMENT 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) KIDS DISCOVER 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. KIDS DISCOVER 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 AGREEMENT. BOCES will provide KIDS DISCOVER with a copy of its policy as soon as practicable following adoption, and KIDS DISCOVER and BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure KIDS DISCOVER's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

KIDS DISCOVER 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 KIDS DISCOVER and is set forth below.

Additional elements of KIDS DISCOVER'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, KIDS DISCOVER will:

Not collect, record, store, or otherwise obtain any Personally Identifiable Information from any users, whether students or teachers or principals, unless it is deemed necessary in order to deliver a purchased solution from Kids Discover. For instance, under Kids Discover Online's Library Media Plan, all usage of the solution is anonymous, utilizing a generic set of building-wide login credentials or IP Authentication. These measures will ensure that Kids Discover is in full compliance with state, federal, and local data security and privacy requirements. For more detail, please refer to the **Data Security and Privacy Plan** provided as an attachment to this Agreement.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the AGREEMENT, KIDS DISCOVER will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the

term of the AGREEMENT:

Please refer to the **Data Security and Privacy Plan** provided as an attachment for more details on Kids Discover's cybersecurity framework, technology stack, safeguards, and protocols for handling Protected Data.

(c) KIDS DISCOVER will comply with all obligations set forth in B OCES "Supplemental Information about the AGREEMENT" 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, KIDS DISCOVER 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 refer to the **Data Security and Privacy Plan** provided as an attachment for more details on how Kids Discover personnel, including contracted workers, are trained and qualified to handle Protected Data.

(e) KIDS DISCOVER [*check one*] __X__ will _____ will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the AGREEMENT. In the event that KIDS DISCOVER engages any subcontractors, assignees, or other authorized agents to perform its obligations under the AGREEMENT, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in BOCES "Supplemental Information about the AGREEMENT," below.

(f) KIDS DISCOVER will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures, and KIDS DISCOVER will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section __B__ of this Data Sharing and Confidentiality Agreement.

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

5. **Additional Statutory and Regulatory Obligations**

KIDS DISCOVER 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 AGREEMENT 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).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist KIDS DISCOVER in fulfilling one or more of its obligations under the AGREEMENT.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of KIDS DISCOVER using the information to carry out KIDS DISCOVER's obligations under the 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 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 AGREEMENT," below.

(g) Provide notification to BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section B of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by KIDS DISCOVER 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 KIDS DISCOVER or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) KIDS DISCOVER 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 KIDS DISCOVER has discovered or been informed of the breach or unauthorized release.

(b) KIDS DISCOVER 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) KIDS DISCOVER 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 KIDS DISCOVER 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 KIDS DISCOVER 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 KIDS DISCOVER representatives who can assist affected individuals that may have additional questions.

(d) KIDS DISCOVER acknowledges that upon initial notification from KIDS DISCOVER, BOCES, as the educational agency with which KIDS DISCOVER contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). KIDS DISCOVER shall not provide this notification to the CPO directly. In the event the CPO contacts KIDS DISCOVER directly or requests more information from KIDS DISCOVER regarding the incident after having been initially informed of the incident by BOCES, KIDS DISCOVER will promptly inform General Counsel or designees.

(e) KIDS DISCOVER 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 B (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.

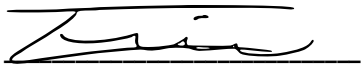
(2) Parents have the right to inspect and review the complete contents of their child's education record.

(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 KIDS DISCOVER:



Signature

President & CEO

Title

4/22/20

Date

EXHIBIT C (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE AGREEMENT BETWEEN
Albany-Schoharie-Schenectady-
Saratoga BOCES AND KIDS DISCOVER

BOCES has entered into An Agreement ("AGREEMENT") with KIDS DISCOVER, LLC ("KIDS DISCOVER"), which governs the availability to Participating Educational Agencies of the following Product(s):

KIDS DISCOVER Exams

Pursuant to the AGREEMENT, Participating Educational Agencies may provide to KIDS DISCOVER, and KIDS DISCOVER 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 be completed by KIDS DISCOVER:

The exclusive purpose for which KIDS DISCOVER is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. KIDS DISCOVER agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the AGREEMENT. Protected Data received by KIDS DISCOVER, or any of KIDS DISCOVER'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 KIDS DISCOVER engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (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 KIDS DISCOVER under the AGREEMENT and applicable state and federal law. KIDS DISCOVER will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by:

Please refer to the **Data Security and Privacy Plan** provided as an attachment for more details on how Kids Discover personnel, including contracted workers, are trained and qualified to handle Protected Data.

Duration of AGREEMENT and Protected Data Upon Expiration:

- The AGREEMENT commences on 4/15/20 and expires on 6/30/23. Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, KIDS DISCOVER will securely delete or otherwise destroy any and all Protected Data remaining in the possession of KIDS DISCOVER or its assignees or subcontractors. If requested by a Participating Educational Agency, KIDS DISCOVER will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion.
- At BOCES request, KIDS DISCOVER will cooperate with BOCES as necessary in order to transition

Protected Data to any successor KIDS DISCOVER(s) prior to deletion.

- KIDS DISCOVER 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, KIDS DISCOVER 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 KIDS DISCOVER, 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 KIDS DISCOVER by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data KIDS DISCOVER receives will be stored on systems maintained by KIDS DISCOVER, or by a subcontractor under the direct control of KIDS DISCOVER, in a secure data center facility located within the United States. The measures that KIDS DISCOVER 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: KIDS DISCOVER (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.

Kids Discover, LLC
192 Lexington Avenue
New York, NY 10016
Phone: (212) 677-4457

April 15, 2020

Data Security and Privacy Plan: Kids Discover Online
Amended for New York State

Introduction

The purpose of this document is to outline the various technologies, safeguards, and business practices that Kids Discover, LLC (Kids Discover, the Company) employs in order to appropriately handle and protect any and all student data or teacher or principal data the Company may receive in conjunction with the services it offers. When reading this document, it is important to note that Kids Discover Online, the digital platform the Company offers its services through, collects a minimal amount of Personally Identifiable Information (as defined below). In some instances, Kids Discover Online may not collect any Personally Identifiable Information in order to provide its full suite of services to School Districts and Educational Agencies, particularly when services are delivered to school library systems. Any questions, inquiries, or clarifications regarding this document should be directed to questions@kidsdiscover.com, and a Kids Discover Representative will reply in a timely manner.

Definitions

1. As it pertains to this Data Security and Privacy Plan, in accordance with New York State Education Law 2-d, the following terms shall have the following meanings:
    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 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. 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.
    d. Educational Agency means a school district, board of cooperative educational services (BOCES), school, or the Department.
    e. 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.
    f. Parent means a parent, legal guardian, or person in parental relation to a student.
    g. 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 Education Law §3012-c (10).
    h. School means any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law §3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law §4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

i. Student means any person attending or seeking to enroll in an educational agency.
j. Student Data means personally identifiable information from the student records of an educational agency.
k. 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 Education Law §§3012-c and 3012-d.

Data Security Framework and Protocols:

Cybersecurity Risk Assessment and Management

- Cybersecurity comes in all shapes and sizes. It is wholly dependent on the type and amount of data that is being collected, managed, stored, and utilized in order to deliver a particular service. Kids Discover Online offers an online library of science, social studies, and nonfiction reading for elementary and middle school aged students. In order to provide this service, Kids Discover Online requires a minimal amount of student data or teacher or principal data. In some instances, Kids Discover Online may not require the collection of any student data or teacher or principal data whatsoever.
    - Collecting a minimal amount of student data or teacher or principal data is the first step in mitigating cybersecurity risk.
    - This minimal amount of collected data also simplifies Kids Discover's management and protection of such data, and therefore informs the software, hardware, and overall systems in place to achieve strong, reliable cybersecurity.
    - It also informs the limited number of Kids Discover personnel that have (and need) access to such data at any given time, along with the extent of proper training that those individuals receive.

Data Collection and Protection

- The Personally Identifiable Information that Kids Discover Online may collect is limited to the following student data or teacher or principal data:
    - Student Data PII
        - First Name and Last Name
            - NOTE: Kids Discover Online does not collect student email addresses, and explicitly prohibits the collection of Student PII other than First and Last Name. For example, NONE of the following examples of Student PII are collected:
                - Name of student's parent or other family members
                - The physical address of the student or student's family
                - A personal identifier, such as student's social security number or student number
                - Student's date of birth
                - Student's attendance
    - Teacher or Principal PII
        - First Name and Last Name
        - Email Address
        - Job Title or Role
        - School Building Name and Address, including Zip Code
            - Kids Discover Online explicitly prohibits the collection of any other personally identifiable information for any Teacher or Principal that uses the service.
- Student data or teacher or principal data that is collected by Kids Discover Online and used to provide the services are protected in the following ways:
    - Access to any and all student data or teacher or principal data is limited to authorized Kids Discover personnel, and requires Company issued credentials that are updated every 3 months. The number of Kids Discover personnel with authorization is limited to individuals that have received proper training, and fully understand their roles and responsibilities.

        - All authorized personnel have received training from IT professionals and senior executives at Kids Discover.
        - Authorized personnel in charge of the development, management, maintenance, and overall support of critical systems, software, and hardware that stores such data are IT professionals with graduate degrees and extensive training in IT and Cybersecurity Operations.
    - Student data or teacher or principal data that is collected by Kids Discover Online is stored in a cloud managed, enterprise grade Microsoft Azure SQL Server Database. The database utilizes the SHA1 hashing algorithm, with a hash sequence of 160 bits in length.
        - Data is automatically backed up every 24 hours.
        - Database capacity is 250GB, more than double the capacity needed to effectively store and run its contents.
        - Kids Discover Online utilizes three different development environments, including a local environment, staged environment, and production environment for both the database and general code base of the platform. This ensures that any testing, enhancements, bug fixes, data handling and/or data conversions are executed in two different test environments before being executed in a production environment (with live data).
        - Data that has been dormant for 12 months is automatically deleted from the database.
            - Data can be deleted within 24 to 48 hours by written request from any School, School District, Educational Agency, or Customer.
            - Data can be provided and delivered to any School, School District, Educational Agency, or Customer within 24 to 48 hours by written request.
    - Kids Discover Online's database is virtually managed. Updates and upgrades are performed through Kids Discover's Microsoft Azure account, utilizing Microsoft Azure's market leading infrastructure and resources.

Systems Monitoring and Detection

- Kids Discover utilizes a suite of tools afforded by Microsoft Azure to monitor, detect, and in turn alert Kids Discover personnel of any anomalous activity.
    - Examples of anomalous activity may include, but are not limited to:
        - Traffic spikes from non-customer IP addresses
        - Service interruptions
        - Elevated levels of server errors
        - Brute force attacks
        - Microsoft-issued systems updates
    - Kids Discover personnel are alerted in real-time to anomalous activity based on predetermined thresholds and triggers. Depending on the nature of the anomalous activity and subsequent alert, Kids Discover personnel are clear in their roles and responsibilities in terms of response time and prioritization.

Response and Recovery

- Once an anomaly is detected, authorized Kids Discover personnel will conduct an investigation that includes, but is not limited to:
    - Review and analysis of server logs
    - Review and analysis of database contents
    - System performance tests and security audits
- Information is then shared to the appropriate Kids Discover personnel, including Kids Discover Management, to determine the depth and magnitude of any further investigations and potential data recovery procedures needing to be conducted.
- If it is determined that an incident such as a data breach has occurred, and that any data may have been effectively altered or compromised from the resulting incident, Kids Discover personnel will

then notify any customers, Schools, or Educational Agencies as defined in this document of the nature of the incident, whose data may have been affected.
    - It is important to note that Kids Discover views all customers as partners and will work diligently to communicate transparently to all stakeholders of any issues or incidents that have arisen.
    - Kids Discover will continue to communicate with any customers, Schools, or Educational Agencies until the issue has been resolved and rectified, and both parties agree about the best possible path forward.
- Kids Discover will then work to restore, retrieve, correct, and improve any and all affected data, along with the systems, software, hardware, and general processes that resulted in the situation.