EXHIBIT D

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 Erie 1 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 Erie 1 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 Erie 1 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 Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 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 Erie 1 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 Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(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: a comprehensive Information Security Program that continuously monitors and mitigates risk to Protected Data privacy and security, including no less than annual security and privacy training of all employees; utilization of "least privilege" principle for access to Protected Data; and industry standard encryption, system monitoring, code

reviews, and automated testing to protect Protected Data, systems, networks and IT infrastructure.

(c) Vendor will comply with all obligations set forth in Erie 1 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: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor _____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 Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 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 Erie 1 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).

(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 the MLSA.

(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 Vendor using the information to carry out Vendor's obligations under the MLSA, 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 Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 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 Erie 1 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 Erie 1 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 Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or 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 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, Erie 1 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 Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her 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 D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the 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 the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, 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 should be directed in writing to the 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**.

BY THE VENDOR: SCOIR, INC.

Signature

Kevin McCloskey
Printed Name

President
Title

April 14, 2022
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND SCOIR, INC.

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Scoir, Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

Scoir's College Guidance Management System

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: 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 limiting any such disclosures of Protected Data to only those subcontractors, assignees, or other authorized agents that require Protected Data to fulfill their contractual obligations with Scoir and by ensuring all Protected Data is encrypted and only accessible over encrypted SSL/TLS channels user authentication.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on April 15, 2022 and expires on June 30, 2025.
- 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 or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back

to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- 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 Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data 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 its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with 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.

SCOIR

DATA PRIVACY AND SECURITY PLAN

Last Updated: January 6, 2022

This Data Privacy and Security Plan (the "**Plan**") forms a part of and is incorporated into the Client Services Agreement between Scoir, Inc. ("**Provider**"), and Customer, as defined herein. All capitalized terms not defined herein shall have the meaning set forth in the Client Services Agreement.

ARTICLE I: DEFINITIONS

"Applicable Law" means the federal and state statutes and regulations applicable to Customer Data and Student Data including the following, to the extent applicable: Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g ("**FERPA**"); Children's Online Privacy Protection Act, 15 U.S.C. § 6501-6502 ("**COPPA**"); Protection of Pupil Rights Amendment, 20 U.S.C. 1232h ("**PPRA**"); Individuals with Disabilities Education Act, 20 U.S.C. § 1400 *et seq.* ("**IDEA**"); and each specifically applicable state regulation, as provided in Exhibit A.

"Customer" means the educational institution, local educational agency, school administrative unit, education industry association, company, or other legal or professional entity that utilizes or intends to utilize the Services.

"De-Identified Information" means data from which all Personally Identifiable Information has been removed or obscured in a way that reasonably removes the risk of disclosure of the identity of the individual and information about them (e.g., by blurring, masking, or perturbation). De-identification should ensure that any information when put together cannot reasonably indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. Information cannot be de-identified if there are fewer than twenty (20) students in the samples of a particular field or category, e.g., fewer than twenty students in a particular grade or fewer than twenty students of a particular ethnicity.

"Personally Identifiable Information" means any Student Data and metadata obtained by reason of the use of the Services, whether gathered by Provider or provided by Customer or its Invitees. Personally Identifiable Information includes, without limitation, indirect identifiers that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this Plan, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

"School Official" means, consistent with 34 CFR 99.31(a)(1)(i)(B), a contractor that: (1) performs an institutional service or function for which the agency or institution would otherwise use employees; (2) is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) is subject to 34 CFR 99.33 governing the use and re-disclosure of Personally Identifiable Information from student records.

"**Services**" means the online college search, guidance, application, and admissions management services provided or made available by Provider through the website **https://app.scoir.com**, including any subdomain thereof, and all associated mobile applications

"Student Data" means any Personally Identifiable Information, whether gathered by Provider or provided by Customer or its Invitees, that is descriptive of Customer's student Invitees, including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents student identifies, search activity, photos, voice recordings or geolocation information. Student Data includes Student Records and Student-Generated Content (to the extent identifiable to a User) for the purposes of this Plan and for the purposes of Applicable Law. De-Identified Information or anonymous usage data regarding a User's use of the Services shall not be considered Student Data.

"Student-Generated Content" means materials or content created by a student during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

"Student Records" means (1) any information that directly relates to a student that is maintained by Customer; and (2) any information acquired directly from a student through the use of instructional software or applications assigned to the student by Customer or its Invitees.

"Subprocessor" means a Third Party that Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to Personally Identifiable Information.

"Targeted Advertising" means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the Services by such student or the retention of such student's online activities or requests over time.

"Third Party" means an entity that is not Provider or Customer.

ARTICLE II: PURPOSE AND SCOPE

1. **Purpose**. The purpose of this Plan is to describe the duties and responsibilities to protect Student Data transmitted to Provider from the Customer pursuant to the Agreement, including compliance with Applicable Law. In performing the Services, to the extent Personally Identifiable Information from Student Data is transmitted to Provider from Customer, Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the Customer. Provider shall be under the direct control and supervision of the Customer.

2. **Nature of Services Provided**. Provider has agreed to provide the Services described in the Agreement.

3. **Student Data to Be Provided**. In order to perform the Services described in this Article and the Agreement, Customer or Invitees may provide some or all of the data described in the Schedule of Data, attached hereto as Exhibit B.

4. **Governing Terms**. In the event of a conflict with the Agreement, the terms and conditions of this Plan shall prevail with regards to the subject matter hereof.

ARTICLE III: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of Customer**. All Student Data transmitted to Provider pursuant to this Plan is and will continue to be the property of and under the control of the Customer or the party who provided such data (such as the Invitee). Provider further acknowledges and agrees that all copies of such Student Data transmitted to Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Plan in the same manner as the original Student Data. The parties agree that as between them, all rights, including all Intellectual Property Rights in and to Student Data contemplated pursuant to this Plan shall remain the exclusive property of the Customer. For the purposes of Applicable Law, Provider shall be considered a School Official, under the control and direction of Customer as it pertains to the use of Student Data notwithstanding the above. Provider may transfer certain Student Data to a separate account according to the procedures set forth below.

2. **Parent Access**. Customer shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data maintained by Provider, correct erroneous information, and procedures for the transfer of Student-Generated Content to a personal account, consistent with the functionality of the Services. Provider will cooperate and respond within five (5) days to Customer's request to view or correct Student Data maintained by Provider. In the event that a parent of a student or other individual contacts Provider

to review any of the Student Records or Student Data accessed pursuant to the Services, Provider shall refer the parent or individual to the Customer, and Customer will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Provider shall transfer Student Data transmitted to Provider by a student to a separate User account for each student Invitee upon termination of the Agreement or a student's earlier graduation from Customer; provided, however, that such transfer shall only apply to such Student Data that is severable from the Services.

4. **Third Party Request**. Should a Third Party, including, but not limited to law enforcement, former employees of the Customer, current employees of the Customer, and government entities, contact Provider with a request for Student Data held by Provider pursuant to the Services, Provider shall, to the extent permitted by Applicable Law, redirect the Third Party to request the Student Data directly from the Customer and shall cooperate with the Customer to collect the required information. Provider shall notify the Customer in advance of a compelled disclosure to a Third Party, unless legally prohibited. Provider will not disclose, lend, lease, transfer, or sell the Student Data and/or any portion thereof to any Third Party or allow any Third Party to use the Student Data and/or any portion thereof, without the express written consent of the Customer or without a court order or lawfully issued subpoena. Student Data shall not include De-Identified Information or anonymous usage data regarding a student's use of the Services.

5. **No Unauthorized Use**. Provider shall not use Student Data for any purpose other than as explicitly specified in this Plan.

6. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this Plan, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this Plan.

ARTICLE IV: DUTIES OF CLIENT

1. **Privacy Compliance**. Customer shall provide Student Data for the purposes of the Plan in compliance with Applicable Law.

2. **Annual Notification of Rights**. If Customer is subject to FERPA, then Customer shall ensure that its annual FERPA notice designates Provider as a "School Official" pursuant to 34 CFR § 99.31(a)(1)(i)(B) and that, in providing the Services, Provider has a "legitimate educational interest" pursuant to 34 CFR §99.7(a)(3)(iii).

3. **Unauthorized Access Notification**. Customer shall notify Provider promptly of any known or suspected unauthorized access. Customer will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE V: DUTIES OF PROVIDER

1. **Privacy Compliance**. Provider shall comply with all Applicable Law with respect to the privacy and security of Student Data and the handling of any breach or unauthorized release of Personally Identifiable Information.

2. **Authorized Use**. Student Data shared pursuant to this Plan, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this Plan, as authorized by Customer, or as authorized by the applicable student or parent. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, any meta data, user content or other non-public information and/or Personally Identifiable Information contained in the Student Data, unless the Customer has given express written consent, it is De-Identified Information, or this Plan otherwise allows its disclosure.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this Plan with respect to the data shared under this Plan. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Plan.

4. **No Disclosure**. De-Identified Information may be used by Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify De-Identified Information and not to transfer De-Identified Information to any party unless (a) that party agrees in writing not to attempt re-identification, or (b) prior written notice has been given to the Customer who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under this Plan and/or any portion thereof, except as necessary to fulfill the Plan.

5. **Disposition of Data**. Provider shall dispose, delete, or de-identify, in accordance with NIST Special Publication 800-88, all Personally Identifiable Information obtained under the Plan when it is no longer needed for the purpose for which it was obtained. If requested by Customer prior to such disposition, Provider shall first transfer a copy of said data to Customer, or Customer's designee, according to a schedule and procedure reasonable agreed between the parties. Nothing in the Plan authorizes Provider to maintain Personally Identifiable Information beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to Customer when the data has been disposed. The duty to dispose of Student Data shall not extend to De-Identified Information or data placed in a separate User account, pursuant to the other terms of the Plan.

6. **Advertising Prohibition**. Provider is prohibited from using Student Data to (a) inform, influence, or enable Targeted Advertising to students or families/guardians; (b) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Services; or (c) develop commercial products or services unrelated to the Services provided to Customer.

ARTICLE VI: DATA PROVISIONS

1. **Data Security**. Provider agrees to maintain and abide by a comprehensive information security program that includes appropriate administrative, technological, and physical safeguards consistent with industry best practices to protect the security, privacy, confidentiality, and integrity of Student Data. General security duties of Provider are as follows:

    a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall, where permissible by law, be subject to criminal background checks.

    b. **Security Protocols**. Each party agrees to maintain security protocols that meet industry practices regarding the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall not copy, reproduce, or transmit data obtained pursuant to the Plan, except as necessary to fulfill the purpose of data requests by Customer. The foregoing does not limit the ability of Provider to allow any necessary service providers to view or access data as provided in this Agreement.

    c. **Employee Training**. Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide Customer with contact information of an employee who Customer may contact if there are any security concerns or questions.

d. **Security Technology**. When the Services are accessed using a supported web browser, Secure Socket Layer or equivalent technology shall be employed to protect data from unauthorized access. The Services security measures shall include server authentication and data encryption. All data shall be encrypted in transmission and at rest in accordance with NIST Special Publication 800-57, as amended. Provider shall host all Services data in SOC 2 compliant environments located within the United States of America.

e. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article VI and in accordance with Applicable Law. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

f. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

g. **Backups**. Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.

h. **Audits**. Upon receipt of a reasonable request from the Customer, Provider will allow the Customer to audit, at Customer's expense, the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof. Provider will cooperate fully with the Customer and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of Provider and/or delivery of Services to students and/or Customer, and shall provide full access to Provider's facilities, staff, agents and Customer's Student Data and all records pertaining to Provider, Customer and delivery of Services to Provider.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall notify Customer within a reasonable amount of time of its discovery of the incident, not to exceed forty-eight (48) hours. Provider shall follow the following process:

   a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What Provider Are Doing," "What Customer Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

   b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

      i. The name and contact information of the reporting Customer subject to this section.

      ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

      iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

      iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

      v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

      vi. Information about what Provider has done to protect individuals whose information has been breached.

vii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

c. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including Personally Identifiable Information and agrees to provide Customer, upon request, with a copy of said written incident response plan.

d. Only upon the written request of, and with the assistance of, Customer shall Provider notify the affected Invitee of the unauthorized access, which notice shall include the information listed in subsection (b) above.

[Remainder of page intentionally left blank.]

EXHIBIT "A": APPLICABLE STATE LAW

If Customer is located in:	the following laws will be included in "Applicable Law":
Arizona	Ariz. Rev. Stat. § 15-1046
Arkansas	AR Code § 6-18-109, Student Online Personal Information Protection Act ("SOPIPA")
California	Cal. Ed. Code § 49073.1 Cal. Bus. & Prof. Code § 22584, Student Online Personal Information Protection Act ("SOPIPA") Cal. Civ. Code § 1798.82
Colorado	C.S.R. §§ 22-16-108 through 22-16-111, Student Data Transparency and Security Act ("SDTSA")
Connecticut	Conn. Gen. Stat. §§ 10-234aa through 10-234dd
Delaware	Del. Code tit. 14 § 81A, Student Data Privacy Protection Act
District of Columbia	DC Code § 38-831.01 – 38-831.02
Florida	Fla. Stat. § 1001.41 Fla. Stat. § 1002.22
Georgia	GA Code § 20-2-666
Hawaii	HI Rev. Stat. § 302A 499-500, Student Online Personal Information Protection Act ("SOPIPA")
Idaho	Idaho Code § 33-133
Illinois	105 Ill. Comp. Stat. § 10, Illinois School Student Records Act ("ISSRA") 105 Ill. Comp. Stat. § 85, Student Online Personal Protection Act ("SOPPA")
Iowa	IA Code § 279.70, Student Online Personal Information Protection Act ("SOPIPA")
Kansas	Kan. Stat. § 72.6331 *et seq.*, Student Online Personal Protection Act ("SOPPA")
Kentucky	Ky. Rev Stat § 365.734
Louisiana	La. Rev. Stat. § 17:3914 La. Rev. Stat. § 51:3071 *et seq.*
Maine	Me. Rev. Stat. tit. 20 § 951 *et seq.*, the Student Information Privacy Act ("SIPA")
Maryland	MD Educ. Code § 4-131
Massachusetts	603 Code Mass. Regs. 23.00, Student Records Mass. Gen. Laws ch. 71, §§ 34D - 34H
Michigan	Mich. Comp. Laws §§ 388.1291 – 388.1295, Student Online Personal Protection Act ("SOPPA")
Nebraska	NE Code § 79-2,153 – 79-2,155, Student Online Personal Protection Act ("SOPPA")
Nevada	NV Rev Stat § 388.281 – 388.296
New Hampshire	NH Rev. Stat. § 189:1-e NH Rev. Stat. § 189:65 through 189:68-a

New York	N.Y. Ed. Law § 2-d
North Carolina	N.C. Gen. Stat. § 115C-401.2, Student Online Privacy Protection Act ("SOPPA")
Oregon	Or. Rev. Stat. § 336.184, Oregon Student Information Protection Act ("OSIPA") Or. Rev. Stat. § 326.565, *et seq.*
Rhode Island	R.I. Gen. Laws § 16-104-1
Tennessee	Tenn. Code Ann. § 49-1-708, Student Online Personal Protection Act ("SOPPA")
Texas	Tex. Ed. Code ch. 32 §§ 151-157
Utah	Utah Code § 53E-9-301 *et seq.*
Virginia	Va. Code § 22.1-289.01
Washington	Wash. Rev. Code § 19.255.010 Wash. Rev. Code § 28A.604, Student User Privacy in Education Rights ("SUPER") Act Wash. Rev. Code § 42.56.590
Wisconsin	Wis. Stat. § 118.125 Wis. Stat. § 134.98

[Remainder of page intentionally left blank.]

EXHIBIT "B": SCHEDULE OF DATA

Category of Data	Elements	Check ("X") indicates potential use in Services
Application Technology Metadata	IP Addresses, Use of cookies etc.	X
	Other application technology metadata: N/A	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	X
	Observation data	
	Other assessment data (specify): *Student Personality & Career Assessments*	X
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information: N/A	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	X
	Specific curriculum programs	
	Year of graduation	X
	Other enrollment information: N/A	
Guardian / Parent Contact Information	Address	X
	Email	X
	Phone	X
Guardian / Parent ID	Parent ID number (created to link parents to students)	X
Guardian / Parent Name	First and/or Last	X
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	

Category of Data	Elements	Check ("X") indicates potential use in Services
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information(specify): *First Generation College Student*	X
Student Contact Information	Address	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	X
	State ID number	
	Vendor/App assigned student ID No.	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In-App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures etc.	X
	Other student work data: N/A	
Transcript	Student course grades	X
	Student course data	X
	Student course grades/performance scores	X
	Other transcript data Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data: N/A	
Other	None	