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. For the avoidance of doubt, Protected Data does not include De-identified Data, as defined in the MLSA.

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: Please see the attached Data Handling and Privacy Statement.

(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 [*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 Erie 1 BOCES' "Supplemental Information about the MLSA," below. For the avoidance of doubt, sub-contractors shall not include Vendor's cloud hosting provider, and vendors used in the ordinary course of business who perform technology and software development and maintenance services under Vendor's supervision on Vendor's internal systems

(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 and written request is received from the applicable Participating Educational Agency, 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. For the avoidance of doubt, De-identified Data may be used by Vendor for product development, product functionality and research purposes, as allowed under FERPA.

(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:

DocuSigned by:
Robert Waldron
4CBC6DFAA10B40C...
Signature

Robert Waldron
Printed Name

Chief Executive Officer
Title

5/22/2023
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND CURRICULUM ASSOCIATES, LLC

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

i-Ready®

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: Vendor will not be using subcontractors to perform under the MLSA.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal and written request by Erie 1 BOCES, or upon termination of the MLSA prior to expiration and written request by Erie 1 BOCES, 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 with the exception of backups, which are automatically deleted over time in accordance with Vendor's data retention and destruction policies. If requested in writing 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, with the exception of backups as noted above.

- 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.

i-Ready® Platform
Data Handling and Privacy Statement
Last Updated: October 21, 2021

Purpose. Curriculum Associates ("CA") takes the protection of our customers' data and information, particularly student data, very seriously. The purpose of this Data Handling and Privacy Statement is to inform our customers about our current data security policies and practices, which are intended to safeguard this sensitive information. CA handles customer data in a manner consistent with applicable laws and regulations, including, without limitation, the Federal Family Educational Rights and Privacy Act (FERPA), the California Student Online Personal Information Protection Act (SOPIPA), the Children's Online Privacy Protection Act (COPPA), the California Consumer Privacy Act, and other state student data privacy protection laws.

Scope. This policy covers the collection, use, and storage of data that is obtained through the use of the products and related services accessible through the use of CA's proprietary i-Ready® platform, i-Ready Connect™. These include i-Ready® Assessment, i-Ready Learning, i-Ready Learning Games, i-Ready Standards Mastery, i-Ready reports and reporting tools, and the e-book versions and digital components of Ready Classroom™ Mathematics. All of these products and services are collectively referred to in this policy as "i-Ready." Note that there are separate terms applicable only to i-Ready Teacher Toolbox, an educator-only facing product. These separate terms are described at the end of this privacy statement.

Student Data Obtained and Collected.
CA receives certain information, which we receive pursuant to the school official exception under FERPA, from its school district customers to enable students to use i-Ready. The following information is generally provided to CA for each student user of i-Ready:
• student first and last name;
• date of birth;
• gender;
• ethnicity or race;
• student identification number;
• student school or class enrollment;
• student grade level;
• teacher name;
• English language learner status, and;
• eligibility for free- or reduced-price lunch.

Note that some of these data fields (such as ethnicity or race, ELL status, eligibility for free or reduced- price lunch) are not required for the use of i-Ready. However, where districts would like reporting capabilities based on these categories, they may choose to provide this information to CA.

Data We Do Not Collect.
CA never obtains or collects the following categories of information through the use of i-Ready:
• user biometric or health data;
• user geolocation data;

• student email addresses or social media profile information; or
• student mailing addresses or phone numbers, or other such “directory” information.

Usage Data.
When students use i-Ready, certain assessment results and usage metrics are also created. These results and usage metrics are used by CA as described below. While teachers and school administrators are able to access student information and related i-Ready usage data, this information is not made available to other students or the public.

How We Use Student Data. CA only uses student data for education-related purposes and to improve teaching and learning, as described in more detail here. We receive this data under the “school official” exception under FERPA:

• **For Services**. CA only uses student-identifiable data provided by schools and/or school districts to make i-Ready available to that particular student, and to provide related reports and services to that student’s school and school district and its educators and administrators. CA uses student data collected from the use of i-Ready for the purpose of making i-Ready available to its customers and for improving its content and effectiveness.

• **For Reporting**. CA provides reporting capabilities to its educator customers, and these reports are generated based on i-Ready usage information.

• **For Account Support**. Customers’ usage data may also be used on an aggregated basis to allow CA’ account management, customer service and tech support teams to provide services that meet the specific needs of our educator customers.

• **Treatment as PII**. CA treats all student-identifiable data, and any combination of that data, as personally-identifiable information, and that data is stored securely as described more fully below.

• **No Solicitation of Students**. CA receives education records from our school district customers to enable students and teachers to use i-Ready. CA does not solicit personally identifiable information directly from students—all student information is provided by school district customers or created through the use of the i-Ready platform. Because i-Ready is only used in the context of school-directed learning, schools are not required to obtain parental consent under COPPA to provide us with this data, although many customers choose to do so to comply with state or local requirements.

• **No Ownership**. CA does not obtain any ownership interest in student-identifiable data.

How We Use De-Identified Data.
• CA collects and uses “de-identified student data”, which refers to data generated from usage of i-Ready from which all personally identifiable information has been removed or obscured so that it does not identify individual students and there is no reasonable basis to believe that the information can be used to identify individual students.
• CA uses this aggregated, de-identified student data for core product functionality to make i-Ready a more effective, adaptive product.

• CA uses de-identified data to provide services to our educator customers. We sometimes use third party software tools (such as Salesforce or Domo) to enhance the level of service we provide. However, we only use de-identified data with these tools.
• CA also uses de-identified student and educator data for research and development purposes. This might include research analyzing the efficacy of i-Ready or development efforts related to our product and service offerings. We also conduct research using de-identified data for studies focused on improving educational systems and student outcomes more generally.
• While some of this research work is done internally, CA does share de-identified student data with trusted third-party research partners as part of these research initiatives.
• CA does not attempt to re-identify de-identified student data and takes reasonable measures to protect against the re-identification of its de-identified student data.
• Our research partners are prohibited from attempting to re-identify de-identified student or educator data.
• CA does not sell student identifiable data or aggregated de-identified student or educator data to third parties.

No Targeted Advertisements or Marketing.
• CA does not include advertisements or marketing messages within i-Ready nor does it use student data for targeted advertising or marketing.
• No student data collected in connection with i-Ready usage is shared with third parties for any advertising, marketing, or tracking purposes.

No User Interactions.
• There are no social interactions between users in i-Ready, and a given user's account is not accessible to other student users or third parties. Thus there is no opportunity for cyberbullying within i-Ready.
• There is no ability for users to upload user content created outside of i-Ready. Other than responses to questions or instructional prompts, students cannot create content within i-Ready
• i-Ready user information does not involve the creation of a profile, and cannot be shared for social purposes.

Student Privacy Pledge. To further demonstrate its commitment to protecting the privacy of student information, CA has taken the Student Privacy Pledge https://studentprivacypledge.org/. This means that, among other things, CA has pledged not to sell student information, not to engage in behaviorally targeted advertising, and to use collected data for authorized purposes only. CA only uses collected student data for the purposes described in the "How We Use Student Data" paragraph.

How We Use Educator Data. CA also collects the following information about educators that use the i-Ready platform: name, school or district affiliation, grade level teaching, IP address, and email address. CA uses this information for account registration and maintenance purposes. CA also records when educator account logins are created, and when educators log in and out of the i-Ready platform. CA utilizes a third-party service provider to host professional-development content for educators in a learning-management system (LMS). For any educator who utilizes that content, CA and/or the educator will provide certain i-Ready account information to its third-party service provider, and this information will be used to communicate with educators and district-level administrators more effectively about their specific implementation, and to better understand how educators use the i-Ready and LMS platforms.

We may also use de-identified educator data to improve our product and service offerings, as described in the "How We Use De-Identified Data" section above.

Data Storage Location.
• i-Ready is a cloud-based application.
• Our servers are located in Tier 1 data centers located in the United States.
• We do not store any student data outside of the US.

Network-Level Security Measures.
• CA's i-Ready systems and servers are hosted in a cloud environment.
• Our hosting provider implements network-level security measures in accordance with industry standards.
• Curriculum Associates manages its own controls of the network environment.

Server-Level Security Measures.
• Access to production servers is limited to a small, identified group of operations engineers who are trained specifically for those responsibilities.
• The servers are configured to conduct daily updates for any security patches that are released and applicable.
• The servers have anti-virus protection, intrusion detection, configuration control, monitoring/alerting, and automated backups.
• Curriculum Associates conducts regular vulnerability testing.

Computer/Laptop/Device Security Measures. Curriculum Associates employs a full IT staff that manages and secures its corporate and employee IT systems. Laptops are encrypted and centrally managed with respect to configuration updates and anti-virus protection. Access to all CA computers and laptops is password-controlled. CA sets up teacher and administrator accounts for i-Ready so that they are also password-controlled. We support customers that use single sign on (SSO) technology for accessing i-Ready.

Encryption.
• i-Ready is only accessible via https and all public network traffic is encrypted with the latest encryption standards.
• Encryption of data at rest is implemented for all data stored in the i-Ready system.

Employee and Contractor Policies and Procedures. CA limits access to student- identifiable data and customer data to those employees who need to have such access in order to allow CA to provide quality products and services to its customers. CA requires all employees who have access to CA servers and systems to sign confidentiality agreements. CA requires its employees and contractors who have access to student data to participate in annual training sessions on IT security policies and best practices. Any employee who ceases working at CA is reminded of his or her confidentiality obligations at the time of departure, and network access is terminated at that time.

Third-Party Audits and Monitoring. In addition to internal monitoring and vulnerability assessments, Curriculum Associates contracts with a third party to conduct annual security audits, which includes penetration testing of the i-Ready application. Curriculum Associates

reviews the third-party audit findings and implements recommended security program changes and enhancements where practical and appropriate.

Data Retention and Destruction. Student and teacher personal data is used only in the production systems and only for the explicitly identified functions of the i-Ready application. Student and teacher personal data is de-identified before any testing or research activities may be conducted. Upon the written request of a customer, Curriculum Associates will remove all personally identifiable student and educator data from its production systems when CA will no longer be providing access to i-Ready to that customer. In addition, CA reserves the right, in its sole discretion, to remove a particular customer's student data from its production servers a reasonable period of time after its relationship with the customer has ended, as demonstrated by the end of contract term or a significant period of inactivity in all customer accounts. Student data is removed from backups in accordance with CA's data retention practices. If CA is required to restore any materials from its backups, it will purge all student-identifiable data not currently in use in the production systems from the restored backups.

Correction and Removal of Student Data.
• Parents of students, guardians, or eligible students who use i-Ready may request correction or removal of the student's personally identifiable data from i-Ready by contacting their student's teacher or school administrator. The teacher or school administrator can then verify the identity of the requesting party and notify CA of the request. • CA will promptly comply with valid requests for correction or removal of student data; however, removal of student personally identifiable data will limit that student's ability to use i-Ready.

Breach Notification.
CA follows documented "Security Incident Management Procedures" when investigating any potential security incident. In the event of a data security breach, CA will notify impacted customers as promptly as possible that a breach has occurred, and will inform them (to the extent known) what data has been compromised. CA expects customers to notify individual teachers and parents of any such breach to the extent required, but will provide customers reasonably requested assistance with such notifications and will also reimburse customers for the reasonable costs associated with legally required breach notices.

Data Collection and Handling Practices for All Teacher Toolboxes.
The Teacher Toolbox for Ready Classroom Mathematics, Ready Mathematics, Ready Reading, and Ready Writing provides a set of digital resources intended for use by educators. It is not a student-facing product, and therefore no student data is collected through the use of any Teacher Toolboxes. CA collects the following information about educators who use a Teacher Toolbox: name, school or district affiliation, grade level teaching, and email address. CA uses this information for account registration and maintenance purposes. CA also records when educator account logins are created, and when educators log in and out of Teacher Toolbox. When a teacher uses a Teacher Toolbox, our systems record which resources have been accessed by whom and the frequency of access. We use this information for product development purposes, to ensure that we are providing educators with resources that are useful to them. Our account management, customer service and tech support teams also use this information to provide more specifically tailored support to our educator customers. Upon request, we may also provide this information to school or district level administrators to help them better understand how our Toolbox resources are used by educators in their school or

district. We also use this information to communicate with educators more effectively about their specific implementation. We do not sell this information or otherwise share it with any third parties, nor do we serve advertisements to educators based on this usage data. We do not use this data to create a profile about any of the educators who use our products to provide to anyone outside of CA. We simply use this collected data for internal purposes to make our product and service offerings better.

Opt-In Google Classroom Assignment Feature for i-Ready Teacher Toolbox.
For districts that use Google Classroom, Curriculum Associates offers educators the ability to easily assign student-facing content from i-Ready Teacher Toolbox to their students through Google Classroom. If an educator elects to utilize this feature, Google Classroom will provide Curriculum Associates with the educator's name and email address, as well as the roster information and coursework data for that educator's classroom. In addition, if permission is granted by the educator, Google will allow Curriculum Associates to access the educator's Google Classroom environment and to directly upload i-Ready Teacher Toolbox content into Google Classroom through Google Drive. Use of Google Classroom is subject to Google Classroom's terms of service and privacy policy.

Policy Review.
Curriculum Associates reviews this privacy policy on an annual basis and makes updates from time to time to reflect changes in legal requirements and to provide more clarity to our customers on our practices. If you have any questions about our data-handling practices or this privacy policy, you may contact us at privacy@cainc.com.

California and Nevada Residents: Visithttps://cdn.i-ready.com/instruction/content/system-check/iReady_Privacy_Policy_CCPA_Addendum.pdffor additional rights applicable to you.