New York

Student Data Privacy and Security Plan

Last Updated: March 4, 2024

Purpose.

Curriculum Associates ("CA") takes the protection of our customers' data and information, particularly student data, very seriously. The purpose of this New York Student Data Privacy and Security Plan is to inform our New York 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), New York Education Law §2-d, as well as other state student data privacy protection laws.

Scope.

This plan 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 Teacher Toolbox, an educator-only facing product. These separate terms are described at the end of this plan.

Student Bill of Rights.

The Parents Bill of Rights for Data Privacy and Security ("Parents Bill of Rights") is attached as Exhibit A.

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 (ELL) 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;
- 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's 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 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 data.
- CA does not sell student identifiable data or aggregated de-identified student 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 at 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, 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.

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 current 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 who use *i-Ready* may request correction or removal of their child's personally identifiable data from *i-Ready* by contacting their child'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.

If you have any questions about our data handling practices or this privacy policy, you may contact us at privacy@cainc.com.

Exhibit A

Parents Bill of Rights for Data Privacy and Security

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by the school district is available from the school district.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints should be submitted directly to the school district.
7. To be notified by the school district in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Curriculum Associates, LLC

By: Stephen Pyne

Name: Stephen Pyne

Title: Vice President and Chief Information Security Officer