

**RHODE ISLAND STUDENT DATA PRIVACY AGREEMENT
VERSION (2022)**

Narragansett School District

and

CK-12 Foundation, U.S. non-profit organization

8/10

_____, 2022

This Rhode Island Student Data Privacy Agreement (“DPA”) is entered into by and between Narragansett School District (hereinafter referred to as “LEA”) and CK-12 Foundation, U.S. non-profit organization (hereinafter referred to as “Provider”) on 8/10, 2022. The Parties agree to the terms as stated herein. This agreement covers only student accounts sanctioned by the LEA and set up through the @ nssk12.org domain(s).

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) as described in Article I and Exhibit “A”, through Provider’s online platform (which consists of Provider’s website located at ck12.org and Provider’s mobile applications), the use of which platform is governed by Provider’s Terms of Use published at www.ck12info.org/terms-of-use/ (the “Service Agreement”); and

WHEREAS, the Provider, by signing this DPA, agrees to allow the LEA to offer school districts in Rhode Island the opportunity to accept and enjoy the benefits of this DPA for the Services described, without the need to negotiate terms in a separate DPA; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

WHEREAS, the documents and data transferred from Rhode Island LEAs and created by the Provider’s Services are also subject to several Rhode Island student privacy laws, including R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

- 1. Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit “C”) transmitted to Provider from the LEA pursuant to Exhibit “A”, including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq. and other applicable Rhode Island state laws. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described in Exhibit “A”.
3. **Student Data to Be Provided.** In order to perform the Services described in this Article and Exhibit “A”, LEA shall provide the categories of data described in the Schedule of Data, attached hereto as Exhibit “B”.
4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this DPA shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. The Provider will cooperate and provide Student Data within ten (10) days at the LEA’s request. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall cooperate and respond within ten (10) days to the LEA’s request for personally identifiable information in a pupil’s records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.

4. **Third Party Request.** Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.
5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws.** LEA shall provide data for the purposes of the DPA in compliance with the FERPA, PPRRA, IDEA, R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq. and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.
4. **Customization of Content and Resources.** LEA shall ensure that any User Content including messages, reviews, photos, videos, images, folders, data, text, and other types of works created by teachers or other LEA personnel and Provider content or resources customized by the LEA, its teachers, or other personnel does not include Student Data.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable Rhode Island and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRRA, R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq. and all other applicable Rhode Island privacy statutes and regulations. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
2. **Authorized Use.** Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as authorized under the statutes referred to in subsection (1), above. 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 student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.
4. **No Disclosure.** De-identified information, as defined in Exhibit “C”, may be used by the 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 Student Data and not to transfer de-identified Student Data to any third party outside of Provider unless (a) that party agrees in writing not to attempt re-identification; and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. For the avoidance of doubt, Provider may share de-identified information with its service providers or research institutions without first obtaining written consent from the LEA, provided that the service providers or research institutions are prohibited from using the de-identified information for purposes other than performing services for the Provider. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA’s written approval of the manner in which de-identified data is presented.
5. **Disposition of Data.** Provider shall dispose or delete all personally identifiable data obtained under the DPA when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA’s designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable.

Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of Student Data shall not extend to: (i) data that has been de-identified or placed in a separate Student account, pursuant to the other terms of this DPA; and (ii) personally identifiable data that was maintained and controlled by Provider prior to the term of this Agreement. The LEA may employ a “Request for Return or Deletion of Student Data” FORM, A Copy of which is attached hereto as Exhibit “D”). Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

- 6. Advertising Prohibition.** Provider is prohibited from leasing, renting, using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.

ARTICLE V: DATA PROVISIONS

- 1. Data Security.** The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit “F” hereto. These measures shall include, but are not limited to:
- 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 NIST 800-53 revision 4. 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 pass criminal background checks.
 - b. Destruction of Data.** Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under this DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA’s designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in this DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition. The duty to dispose of Student Data shall not extend to data that has been de-identified.
 - c. Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in 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 maintain all data obtained or generated pursuant to this DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to this DPA, except as

necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.

- d. Employee Training.** The Provider shall provide recurring, periodic (no less than annual, with additional sessions as needed throughout the year to address relevant issues/changes, such as (but not necessarily limited to) new or evolving security threats, changes to security protocols or practices, changes to software and/or hardware, identified vulnerabilities, etc.) security training to those of its employees who operate or have access to the system. Such trainings must be tailored to the Provider's business and cover, but not necessarily be limited to, the following topics: common types of attackers (e.g., cyber criminals, hacktivists, government sponsored groups, inside threats, etc.); common types of attacks (e.g., social engineering, spoofing, phishing, etc.) and how the information sought is typically used; identifying threats, avoiding threats, physical security and environmental controls; internal policies and procedures; and safe internet habits. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to this DPA in an environment using a firewall that is periodically updated according to industry standards.
- f. Security Coordinator.** Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to this DPA.
- g. 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 V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.
- h. 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.
- i. 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.
- j. Audits.** At least once a year, except in the case of a verified breach, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof, subject to reasonable time and manner restrictions. The Provider will provide reasonable access to the LEA and any state or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA.
- k. Rhode Island Specific Data Security Requirements.** The Provider agrees to continue to adopt technologies, safeguards and practices in alignment with the NIST Cybersecurity

Framework (NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher). The Provider's NIST "Current Profile" is available upon request.

2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within thirty (30) days of confirmation of the incident. 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," "When it Occurred," "What We Are Doing," "What You 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 LEA 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. The estimated number of students and teachers affected by the breach, if any.
 - vii. A clear and concise description of the affected parent, legal guardian, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, or eligible student requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.
 - c. At LEA's discretion, the security breach notification may also include any of the following:
 - i. **Information about what the agency has done to protect individuals whose information has been breached,** including toll free numbers and websites to contact:
 1. The credit reporting agencies
 2. Remediation service providers
 3. The attorney general

information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Miral Shah, Chief Technology and Product Officer
dpo@ck12.org || 650-494-1302
2300 Geng Rd., Suite 150, Palo Alto, CA 94303
Palo Alto, CA 94303

The designated representative for the LEA for this DPA is:

Giulio Lugini, Director of Technology
Narragansett School District
25 Fifth Ave Narragansett, RI 02882
(401) 792-9450
glugini@nssk12.org

6. **Entire Agreement.** This DPA, together with the Service Agreement, (to the extent not conflicting with this DPA), constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
7. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF RHODE ISLAND, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE

STATE AND FEDERAL COURTS OF WASHINGTON COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof is stored, maintained or used in any way.
10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Multiple Counterparts:** This DPA may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this DPA. In proving this DPA, it shall not be necessary to produce or account for more than one such counterpart. These counterparts can include original hard copies with signatures and/or electronically generated copies with signatures. Execution and delivery of this DPA by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).


ARTICLE VII- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this to any other school district who signs the acceptance in said Exhibit. At that time, the agreement will cover student accounts sanctioned by the district under the domain name(s) as noted in Exhibit E.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Rhode Island Student Data Privacy Agreement as of the last day noted below.

NARRAGANSETT SCHOOL DISTRICT

By:  _____ Date: 8/9/22

Printed Name: Giulio Lugini Title/Position: Director of Technology

CK-12 FOUNDATION, U.S. NON-PROFIT ORGANIZATION

By:  _____ Date: 8/10/2022

Printed Name: Miral Shah Title/Position: CTO and CPO

EXHIBIT “A”
DESCRIPTION OF SERVICES

CK-12 provides lessons in STEM and other subject areas and allows teachers to compile and share custom digital assessments, text, and other learning modalities. By assigning CK-12 resources through CK-12 Classes or an integrated learning management system, students can complete work and teachers can see insights and student progress. Additionally, students are able to use the CK-12 platform to fill in gaps and challenge themselves beyond individual assignments.

EXHIBIT “B”

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	yes
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	yes
Assessment	Standardized test scores	no
	Observation data	no
	Other assessment data-Please specify:	Data from CK-12 practice and learning modalities
Attendance	Student school (daily) attendance data	no
	Student class attendance data	no
Communications	Online communications that are captured (emails, blog entries)	Café/Q&A/chat bot (not required)
Conduct	Conduct or behavioral data	no
Demographics	Date of Birth	yes
	Place of Birth	no
	Gender	no
	Ethnicity or race	no

	Language information (native, preferred or primary language spoken by student)	no
	Other demographic information-Please specify:	no
Enrollment	Student school enrollment	yes
	Student grade level	yes
	Homeroom	no
	Guidance counselor	no
	Specific curriculum programs	no
	Year of graduation	no
	Other enrollment information-Please specify:	no
Parent/Guardian Contact Information	Address	no
	Email	yes (for under 13)
	Phone	no
Parent/Guardian ID	Parent ID number (created to link parents to students)	no
Parent/Guardian Name	First and/or Last	no
Schedule	Student scheduled courses	no
	Teacher names	Not as part of a schedule
Special Indicator	English language learner information	no
	Low income status	no

	Medical alerts	no
	Student disability information	no
	Specialized education services (IEP or 504)	no
	Living situations (homeless/foster care)	no
	Other indicator information- Please specify:	no
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	no
	Email	yes (not required)
	Phone	no
Student Identifiers	Local (School district) ID number	no
	State ID number	no
	Vendor/App assigned student ID number	yes
	Student app username	yes
	Student app passwords	yes
Student Name	First and/or Last	yes (not required)
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	yes – student performance on questions and interactions with learning modalities

Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	no
Student Survey Responses	Student responses to surveys or questionnaires	yes (not required)
Student work	Student generated content; writing, pictures etc.	yes
	Other student work data - Please specify:	n/a
Transcript	Student course grades	no
	Student course data	no
	Student course grades/performance scores	no
	Other transcript data -Please specify:	no
Transportation	Student bus assignment	no
	Student pick up and/or drop off location	no
	Student bus card ID number	no
	Other transportation data - Please specify:	no
Other	Please list each additional data element used, stored or collected by your application	

EXHIBIT “C”**DEFINITIONS**

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot 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.

NIST 800-63-3: Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes, without limitation, at least the following:

First Name	Home Address
Last Name	Subject
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	Date of Birth
Grade	Classes
Place of birth	Social Media Address
Unique pupil identifier	
Credit card account number, insurance account number, and financial services account number	
Name of the student's parents or other family members	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student’s Educational Record

Information in the Student's Email

Provider: For purposes of this DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

Pupil Generated Content: The term “pupil-generated content” means materials or content created by a pupil 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 pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is 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(a) governing the use and re-disclosure of personally identifiable information from student records. The definition of “school official” encompasses the definition of “authorized school personnel” under 603 CMR 23.02.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians, that is descriptive of the student 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, the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number, student identifiers, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this DPA, and for the purposes of Rhode Island and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not include the following: (i) any information or content that has been anonymized or de-identified; (ii) anonymous usage data regarding a student’s use of Provider’s services; and (iii) user-generated content that is already published or shared on Provider’s website located at ck12.org and/or through Provider’s mobile applications prior to the Effective Date of this DPA.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider’s General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term “Subprocessor” (sometimes referred to as the “Subcontractor”) means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

Third Party: The term “Third Party” means an entity that is not the Provider or LEA.

EXHIBIT “D”

DIRECTIVE FOR DISPOSITION OF DATA

[Name or District or LEA] directs [Name of Company] to dispose of data obtained by Company pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

___ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

___ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

___ Disposition shall be by destruction or deletion of data.

___ Disposition shall be by de-identification. Notwithstanding any contractual terms previously agreed upon, LEA explicitly gives Provider permission to use de-identified data and use and disclose it for Provider’s own purposes.

___ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date:

___ As soon as commercially practicable

___ By (Insert Date) - (No less than 30 days after the Provider receives this request.)

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

OPTIONAL: EXHIBIT “F”

DATA SECURITY REQUIREMENTS

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy? Yes No

If yes, please provide it. – <https://www.ck12info.org/privacy-policy/>

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

___ ISO 27001/27002

___ CIS Critical Security Controls

___ NIST Framework for Improving Critical Infrastructure Security

X Other: ___NIST Cybersecurity Framework (NIST SP 800-53 rev 4)___

3. Does your organization store any customer data outside the United States? Yes No

4. Does your organization encrypt customer data both in transit and at rest? Yes No

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: ___CK-12 IT Team_____

Contact information: ___dpo@ck12.org_____

6. Please provide any additional information that you desire.



CK12_RI DPA (June 2022) (1)

Final Audit Report

2022-08-09

Created:	2022-08-05
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA29DZ_gZ21DUo3bkywDcEbZWRhue8E_M

"CK12_RI DPA (June 2022) (1)" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2022-08-05 - 3:22:17 PM GMT- IP address: 98.109.87.70
-  Document emailed to Giulio Lugini (glugini@nssk12.org) for signature
2022-08-05 - 3:23:20 PM GMT
-  Email viewed by Giulio Lugini (glugini@nssk12.org)
2022-08-06 - 0:57:59 AM GMT- IP address: 74.125.210.191
-  Document e-signed by Giulio Lugini (glugini@nssk12.org)
Signature Date: 2022-08-09 - 3:01:00 PM GMT - Time Source: server- IP address: 131.109.15.2
-  Agreement completed.
2022-08-09 - 3:01:00 PM GMT