STANDARD STUDENT DATA PRIVACY AGREEMENT

NEW YORK

NY

Arlington Central School District

and

CK-12 Foundation

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Arlington Central School District, located at 144 Todd Hill Rd. Lagrangeville, NY 12540 USA (the "**Local Education Agency**" or "**LEA**") and CK-12 Foundation, located at 4300 Bohannon Drive, Suite 200, Menlo Park, CA 94025, USA (the "**Provider**"). This agreement covers only student accounts sanctioned by the LEA and set up through the @___________________________________ domain(s) for this originating LEA or the noted domain(s) in Exhibit "E" for subscribing LEAs within New York.

WHEREAS, the Provider is providing educational or digital services to LEA.
WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and
WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.
NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   √ If checked, the Supplemental State Terms and attached hereto as **<u>Exhibit "G"</u>** are hereby incorporated by reference into this DPA in their entirety.

   √ If Checked, the Provider, has signed **<u>Exhibit "E"</u>** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between Articles I-VII and the State or Special Provisions, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA and the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in Articles I-VII and the Exhibits attached hereto.

6. **<u>Notices</u>**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Miral Shah, Chief Technology & Product Officer
CK-12 Foundation
4300 Bohannon Drive, Suite 200, Menlo Park, CA 94025
dpo@ck12.org
650-353-4619

The designated representative for the LEA for this DPA is:

Melissa Erlebacher, Chief Communication and
Community Engagement Officer
144 Todd Hill Rd. Lagrangeville, NY 12540
845-486-4460 merlebacher@acsdny.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

Arlington Central School District

By: Melissa Erlebacher
Melissa Erlebacher (Dec 12, 2025 10:39:46 EST)

Date: 12/12/2025

Printed Name: Melissa Erlebacher

Title/Position: Data Protection Officer

CK-12 Foundation

By: DocuSigned by: Miral Shah 81C4BF5FA8444CF...

Date: 11/13/2025

Printed Name: Miral Shah

Title/Position: CTO and CPO

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 including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, 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, with respect to its use of Student Data

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

3. **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 any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the 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**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

5. **User Content**. If teachers or any other LEA staff create user content or customize resources, such teachers or any other LEA staff must not include Student Data in such content or customized resources.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

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

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to (i) aggregate

summaries of De-Identified information, (ii) De-Identified Information disclosed in furtherance of providing Services under the Service Agreement or De-Identified Information disclosed for product development, research, and improvement purposes in furtherance of Provider's mission to increase access to high quality educational materials, or (iii) Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and product development, research, and improvement purposes in furtherance of Provider's mission to increase access to high quality educational materials. Provider's use of De-Identified Data shall survive termination of this DPA and is not subject to any request by LEA to return or destroy Student Data. Except for Subprocessors, and as outlined in Article IV, Section 4, Provider agrees not to transfer de-identified Student Data to any party 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. 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.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request. If LEA fails to submit a written request for deletion within thirty (30) days from termination of this DPA, Provider will remove identifiable Student Data within ninety (90) days of termination. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Article II Section 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services; or (iv) from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate

confidentiality agreement, the Provider will allow the LEA to audit, at LEA's own expense, the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof, subject to reasonable time and manner restrictions and providing minimal disruption to Provider's business, as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The Provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within four (4) business days of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

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

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: 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 **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. This DPA is effective as of the Effective Date specified in the opening paragraph and shall continue until terminated by either party by giving at least thirty (30) days written notice. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Articles I-VII and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service Agreement constitute 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.

5. **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.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party 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.

9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

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. (the "Services")

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.	X
	Other application technology meta data-Please specify: • **approximate location (city/postal code) for content personalization** • **devices and screen sizes for optimal user experience**	X
Application Use Statistics	Meta data on user interaction with application	X
	Standardized test scores	
	Observation data	
	Other assessment data-Please specify: • **user answers / feedback / time / engagement for completion on CK-12 platform**	X
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	X
	Other demographic information-Please specify: • city/state	X
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	

Category of Data	Elements	Check if Used by Your System
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	X

Category of Data	Elements	Check if Used by Your System
Student work	Student generated content; writing, pictures, etc.	X
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application: • Interests/hobbies, major aspirations (for personalization) • Questions and feedback on CK-12 platform	X
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

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

School Official: For the purposes of this DPA 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use. For this DPA, the "Service Agreement" shall be defined as the CK-12 Terms of Use, which are available at the following link:

https://www.ck12info.org/terms-of-use/, which may be updated from time to time. If there is any update, the Parties agree that this DPA controls in the event of a conflict.

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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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 constitute that information that has been anonymized or De-Identified, or anonymous or De-Identified usage data and/or anonymous or De-Identified User Content regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, 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 service, and who has access to Student Data.

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[**Insert Name of District or LEA**] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement 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 a transfer of data. The data shall be transferred to the following site as follows:

[**Insert or attach special instructions**]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By [**Insert Date**] (No fewer than 30 days after the Provider receives this request. If date indicated extends beyond 60 days of the request, Provider shall not be found in violation of Article IV, Section 6 of the DPA.)

4. Signature

_____________________________________ ________________

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____________________________________ ________________

Authorized Representative of Company Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Arlington Central School District** ("Originating LEA") which is dated 12/12/2025, to any other LEA ("Subscribing LEA") from New York who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

privacy-agreements@ck12.org.

CK-12 Foundation

BY: DocuSigned by: Miral Shah 81C4BF5FA8444CF... Date: 11/13/2025

Printed Name: Miral Shah Title/Position: Chief Technology & Product Officer

2. Subscribing LEA

A Subscribing LEA, by agreeing to CK-12's Terms of Use, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA and the accompanying Exhibits with regards to the accounts sanctioned by the LEA under the noted domain(s) for the term of the DPA between the **Arlington Central School District** and the Provider. **This DPA shall become effective on the seventh (7th) day following the date of confirmed receipt of the Subscribing LEA's signature on this offer document by the Provider.**

Subscribing LEA: (School District Name): ______________________

BY: ______________________ Date: ______________________

Printed Name: ______________________ Title/Position: ______________________

SCHOOL DISTRICT DOMAIN(S): ______________________

(e.g. @myschool.com and @student.myschool.org)

DESIGNATED REPRESENTATIVE OF LEA:

Name: ______________________

Title: ______________________

Address: ______________________

Telephone Number: ______________________

Email: ______________________

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	**FRAMEWORK(S)**
X	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit http://www.edspex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"
New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the 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;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

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

1. All employees of the Provider who will have direct virtual or in-person unmonitored contact with students shall pass criminal background checks.
2. Student Data will be used by Provider for no purpose other than the Services outlined in Exhibit A and/or otherwise required under the statutes referred to herein this DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with the Data Security and Privacy Plan set forth in Exhibit K. Each LEA represents that their Data Security and Privacy Policies are materially consistent with Education Law § 2-d. Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data. Provider must Encrypt Student Data at rest and in transit in accordance with applicable New York laws and regulations. Should the LEA or any Subscribing LEA update its Data Security and Privacy Policies to comply with changes in applicable law, the LEA and any subscribing LEA should provide such updates to Provider and work with Provider to update the Data Security and Privacy Plan attached hereto in Exhibit K.
4. Provider represents that their Data Privacy and Security Plan can be found in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all state, federal and local data privacy and security requirements which are (i) applicable to Student Data shared pursuant to the Service Agreement, and (ii) materially consistent with the privacy and security obligations under this DPA; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the Service Agreement; (c) complies with the LEA's Parents Bill of Rights for data privacy and security, provided it is materially consistent with Education Law § 2-d; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data; (e) ensures subprocessors are required to protect PII received under this DPA; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensures prompt notification to the LEA, and (g) addresses Student Data deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J, provided that it is materially consistent with Education Law § 2-d. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and

Privacy to the Provider upon execution of Exhibit "E". Signature on this DPA and Exhibit E serve as signature on the Parents Bill of Rights for the LEA and the Subscribing LEA, respectively.

6. Provider will not provide to CK-12 any APPR Data, and CK-12 does not intend to collect APPR data.
7. To amend **Article II, Section 5** to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data and that they will comply with terms materially consistent with Education Law § 2-d. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point and to Provider's knowledge, a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's Access to Student Data; and (iii) as applicable, retrieve all Student Data received or stored by such Subprocessor and/or ensure that Student Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.
8. In **Article IV, Section 2**, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
9. To amend **Article IV, Section 3** to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data will be trained on the federal and state laws governing confidentiality of such Student Data prior to receipt. Access to or Disclosure of Student Data shall only be provided to Provider's employees and subprocessors who need to know the Student Data to provide the services and such Access and/or Disclosure of Student Data shall be limited to the extent necessary to provide such services.
10. To replace **Article IV, Section 6** (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider's certifying that it and its subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any assurance of discontinuation, which will control in the case of a conflict.

    If LEA fails to submit a written request for deletion within thirty (30) days from termination of this DPA, Provider will remove identifiable StudNent Data within ninety (90) days of termination after providing the LEA notice of the deletion. The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to Article II Section 3. The LEA may employ a **"Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D"**, or other form agreed upon by the parties. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.

11. To amend **Article IV, Section 7** to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data for any Commercial or Marketing Purpose as defined herein.' And add after (iii) account holder, "which term shall not include students."

12. To replace Article V, Section 1 (Data Storage) to state: Student Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designees to audit, at LEA's own expense, the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof, subject to reasonable time and manner restrictions and providing minimal disruption to Provider's business, as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEAand shall provide reasonable Access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. .

    To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education, provided there is no material change. If there is a material change, LEA would have the option, for this reason only, to terminate this DPA with fewer than thirty (30) days notice if Provider was unable to meet the updated requirements by the time they took effect.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within four (4) business days of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident.

    Provider shall follow the following process:
    a. The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
        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; and
        v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
        vi. The number of records affected, if known; and
        vii. A description of the investigation undertaken so far; and
        viii. The name of a point of contact for Provider.

b. Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

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

d. LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of any legally required notification to Parents, Eligible Students, teachers, and/or principals pursuant to NYCRR 121.10(f).).

e. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

f. Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach.
Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- "Provider" is also known as third party contractor. It is any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit "C" the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.

- **APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d

- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.

- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.

- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

- **Release:** Shall have the same meaning as Disclose.

- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.

- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

EXHIBIT "J"
New York LEA Documents

New York LEAs will provide links to their Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement in their Exhibit Es. ONLY LEA Data Security and Privacy Policies, Parents Bill of Rights for Data Security and Privacy, and any supplemental information that are **materially consistent with** Education Law § 2-d should be included. **Provider does NOT agree to comply with LEA policies and security plans and other documents that are not included in Exhibit J and not consistent with** Education Law § 2-d**.**

EXHIBIT "K"
Provider Security Policy & Supplement to the Parents' Bill of Rights

In accordance with its obligations under the Parents' Bill of Rights and Data Privacy and Security Agreement, the Provider verifies the following supplemental information to the Parents' Bill of Rights regarding data privacy and security:

1. The Student Data received by the Provider will be used exclusively for the following purpose(s):

   Provider and its agents, employees and subcontractors, if any, shall use Student Data solely for the purpose of providing services as set forth in the Service Agreement and this DPA. Provider and its agents, employees and subcontractors will not use Student Data for any other purposes. Any Student Data received by Provider or any of its agents, employees, subcontractors or assignees shall not be sold or released for any commercial purposes, nor shall it be sold or used for marketing purposes.

2. The Provider will ensure the confidentiality of Student Data that is shared with subcontractors or other persons or entities as follows:

   In the event that Provider subcontracts with an outside entity or individual in order to fulfill its obligations to the LEA, Provider ensures that it will only share Student Data with such subcontractors who maintain such data privacy and security consistent with those required of Provider pursuant to this DPA. Provider will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Student Data in its custody consistent with the data protection and security requirements of state and federal law and regulations by adhering to the provisions in this Exhibit.

3. This DPA is effective upon execution by both parties and shall continue until terminated by either party by giving at least 30 days written notice. If LEA fails to submit a written request for deletion within thirty (30) days from termination of this DPA, Provider will remove identifiable Student Data within ninety (90) days of termination. Provider will provide written confirmation of such disposition to the LEA, upon written request.

4. A parent, student, teacher or principal can challenge the accuracy of Student Data received by the Provider as follows:

   In the event that a parent or eligible student wishes to challenge the accuracy of Student Data concerning that student that is maintained by Provider or its subcontractors, such challenge may be processed through the procedures provided by the applicable educational agency or institution for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that Provider is notified of the outcome of any such errors made by Provider, it will promptly correct any inaccurate data it or its subcontractors or assignees maintain. The LEA or the applicable New York education agency/institution will use FERPA's data correction procedures, as applicable, to update any data that is not a result of an error made by Provider or its subcontractors.

5. The following is how Student Data will be stored and what security protections will be taken by the Provider:

   All Data in Provider's possession will be securely stored. Provider represents that the following security *protections, including encryption where applicable, will be in place to ensure that Student Data is protected.*

- *Password protections*
- *Administrative procedures*
- *Encryption while Student Data is in motion and at rest*
- *Firewalls*

In accordance with its obligations under the Parents' Bill Rights and Data Privacy and Security Agreement, the Provider represents and warrants that its data security and privacy plan described below contains the following minimum required provisions:

1. Provider will implement state and federal data security and privacy contract requirements for the duration of its contract by:

   Adhering to the NIST Cybersecurity Framework. Our NIST "Current Profile" is available upon request.

2. Provider will use the following administrative, operational and technical safeguards to protect personally identifiable information:

   Refer to Section 13 of the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

3. Provider has complied with requirements of §121.3(c) of the Commissioner's Regulations by providing and complying with the supplemental contractor information as follows:

   §121.3(c)(1)
   - Refer to Section 5 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

   §121.3(c)(2)
   - Refer to Section 6 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

   §121.3(c)(3)
   - For contract duration, refer to item 3 in the Supplement to the Parents' Bill of Rights, above.
   - For disposition or transfer of data, refer to item 3 in the Supplement to the Parents' Bill of Rights, above, and to Sections 8 and 13 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

   §121.3(c)(4)
   - Refer to item 4 in the Parents' Bill of Rights above.

   §121.3(c)(5)
   - The CK-12 site runs on the Amazon Web Services (AWS) cloud.
   - Refer to Section 13 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/, for more information on security.

   §121.3(c)(6)

- Refer to Section 13 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

4. Provider's employees and any assignees with access to student data, or teacher or principal data have received or will receive training on relevant confidentiality laws, before receiving access to such data, as follows:

   Employees with access to Student Data receive training on handling this data.

5. Provider works with third party service providers for cloud-based hosting, communicating with users for product support and information, troubleshooting issues, and analytics.

   For more information on any of the third parties used by Provider, please email: support@ck12.org

6. Provider will implement an action plan for handling any breach or unauthorized disclosure of personally identifiable information and will promptly notify the LEA of any breach or unauthorized disclosure as follows:

   CK-12 has an established incident response plan, which can be provided upon request.

7. Student Data will be returned, transitioned to a successor contractor, deleted, de-identified, or destroyed when the contract ends or is terminated as follows:

   - For disposition or transfer of data, refer to item 3 in the Supplement to the Parents' Bill of Rights, above, and to Section 6 in the CK-12 Privacy Policy, found at https://www.ck12info.org/privacy-policy/

Complete_with_Docusign_CK12_NY_ArlingtonCent_signed

Final Audit Report 2025-12-12

Created:	2025-11-17
By:	TEC SDPA (mmcgrath@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAm_hKRM78KQEQwEllf2MkIsIrFhgBR92-

"Complete_with_Docusign_CK12_NY_ArlingtonCent_signed" History

Document created by TEC SDPA (mmcgrath@tec-coop.org)
2025-11-17 - 1:29:52 PM GMT

Document emailed to Melissa Erlebacher (merlebacher@acsdny.org) for signature
2025-11-17 - 1:30:00 PM GMT

Email viewed by Melissa Erlebacher (merlebacher@acsdny.org)
2025-12-12 - 3:37:30 PM GMT

Document e-signed by Melissa Erlebacher (merlebacher@acsdny.org)
Signature Date: 2025-12-12 - 3:39:46 PM GMT - Time Source: server

Agreement completed.
2025-12-12 - 3:39:46 PM GMT