- Allow the following email domains
  - http://khanacademy.org/
  - http://bounce.khanacademy.org/
  - e.khanacademy.org
  - http://khanacademy.zendesk.com

- Allow the following email addresses
  - districts@e.khanacademy.org
  - schoolpartnerships@e.khanacademy.org
  - teachereducation@khanacademy.org
  - no-reply@khanacademy.org

- Allow the following IP addresses
  - 13.110.236.223
  - 192.64.236.56
  - 192.64.236.57
  - 192.64.237.68
  - 192.64.236.55

- Use the supported internet browsers (Google Chrome, Microsoft Edge, Mozilla Firefox, or Safari, as further detailed above).

- If you are using an AdBlocker like UBlock Origin, Ghostery, or Adblock:
  - Add khanacademy.org to your adblocker's list of allowed or trusted sites.
- If you use Google Workspace for Education
  - Ensure you have an Access Policy with Khan Academy included on it, so students under 18 years old can log in with Google SSO onto Khan Academy
  - Google Workspace for Education + Khan Academy: Guide to configuring an access policy

## EXHIBIT D

Data Sharing and Confidentiality Addendum to the MLSA

INCLUDING

PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

AND

SUPPLEMENTAL INFORMATION ABOUT THE MLSA

DocuSign Envelope ID: DC4A89E5-D55F-4977-BF19-5AC1F06177FB



1. **Purpose**

(a) This Exhibit provides supplemental terms and conditions to the Instructional Technology Free Application RFP response ("RFP") to which it is attached, to ensure that the RFP conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Addendum to the RFP, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the RFP that is required to be posted on Erie 1 BOCES' website (collectively, the "DSA"). This DSA supplements the MLSA and together with the MLSA, is collectively referred to as the "Agreement". Except for the changes made by this DSA, the MLSA remains unchanged and in full force. For clarity, the liability of each party under this DSA shall be subject to the exclusions and limitations of liability set out in the MLSA.

(b) To the extent that any terms contained within the RFP, or any terms contained within any other Exhibits attached to and made a part of the RFP response, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the RFP, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

(c) This DSA will terminate simultaneously and automatically with the termination or expiration of the MLSA. In the event that either party seeks to terminate this DSA, they may do so by terminating the MLSA as set forth therein. Either party may terminate this DSA and the MLSA in the event of a material breach of this DSA by the other party. Notwithstanding the foregoing, statutory obligations under New York Education Law 2-d applicable to Vendor in the provision of the Service shall survive termination.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the RFP will have the same definition as contained within the RFP or MLSA. For clarity, **Exhibit A** to the MLSA describes the Service. Vendor may update the description of the Service from time to time to reflect new products, features, or functionality compromised within the Service. Vendor will update relevant documentation to reflect such changes.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the RFP.

(b) “Teacher or Principal Data” means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the RFP.

(c) “Protected Data” means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor’s Product.

(d) “Participating Educational Agency” means a school district within New York State that purchases (or otherwise obtains access to) certain shared instructional technology services through a Cooperative Educational Services Agreement with a BOCES, and as a result is able to use Vendor’s Product pursuant to the terms of the RFP and the Agreement (including this Exhibit D). The term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor’s Product pursuant to the RFP to support its own educational programs or operations. For the purposes of this DSA, where the Participating Educational Agency is an entity other than Erie 1 BOCES, such Participating Educational Agency expressly assumes and accedes to the obligations of Erie 1 BOCES hereunder; for the avoidance of doubt, each Participating Educational Agency is solely responsible for its own compliance with the terms of the RFP and the Agreement.

(e) “Learning activity” means information relating to an identified student’s use of the Website generated by the user through use of the Website. Learning activity that is De-Identified is not Student Data or personally identifiable information.

(f) “Sell” shall have the meaning assigned by applicable U.S. federal or state law. Sell does not include sharing, transferring or disclosing Student Data with a Subprocessor that is necessary to perform a business purpose (such as detecting security incidents, debugging and repairing, analytics, storage or other processing activities) provided that the Subprocessor does not Sell the Student Data, or any sharing, transfer or disclosure of Student Data made by the user through the functionality of the Services. Sell also does not include or apply to a purchase, merger or other type of acquisition of a company by another entity, provided that the company or successor entity continues to treat the Personally Identifiable Information contained in Student Data in a manner consistent with this DSA with respect to the previously acquired Personally Identifiable Information contained in Student Data.

(g) "Website" means the Khan Academy website and related mobile applications and online services.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the RFP may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates or the party who provided such data (such as the student or parent).

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with applicable federal and state law (including but not limited to Section 2-d) and, to the extent applicable to Vendor, Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy. Erie 1 BOCES will provide Vendor with a copy of its policy and Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this DSA to the extent necessary to ensure Vendor's continued compliance with Section 2-d. Erie 1 BOCES shall provide Vendor with copies of any additional privacy and data security policies or local regulations that are applicable to the Service, and provide Vendor with an opportunity to review and confirm its acceptance of such requirements, or to disclose any variances or exceptions applicable to the Services. Vendor shall not be required to comply with any such policy (i) to the extent inapplicable to the online nature of the Service; or (ii) unless and until Vendor is afforded an opportunity to review and confirm its compliance by expressly accepting such terms in writing.

(c) De-Identified Data may be used by the Vendor for any lawful purpose including, but not limited to, development, adaptive learning and customized student learning, research, and improvement of educational sites, services, and applications, and to demonstrate market effectiveness of the Services. Vendor's use of De-Identified Data shall survive termination of this DSA or any request by Erie 1 BOCES to return or destroy Student Data. Vendor agrees not to attempt to re-identify De-Identified Data retained after termination of the relevant user account.

(d) Nothing in the RFP or the Agreement shall prohibit Vendor, both during and after the term of the Agreement, from collecting or analyzing data received in connection with the Services, as well as data about users' access and use of the Services, for purposes of operating, analyzing, improving, marketing or demonstrating the effectiveness of the Services, developing and improving educational sites, services, or applications, conducting research, or any other

lawful purpose, provided that the data is De-Identified and/or aggregated such that the information does not reasonably identify a specific individual.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this DSA, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that in the provision of their Services they are in conformance with all applicable federal, state, and local laws and the terms of this DSA. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the RFP, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the RFP:

Technical Safeguards.

Encryption of data in transit. Khan Academy employs industry standard encryption technology to protect information and data transmitted over the internet or other public networks.

Data storage and server hosting. Khan Academy utilizes leading secure cloud service providers, and we rely on them for server and datacenter security. The website is hosted on the Google Cloud Platform (GCP). All data on GCP is encrypted at rest in accordance with Google's security practices.

Data access control. Khan Academy uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of

any system resources or user data. Asset owners are responsible for granting access based on the users' role, and access is reviewed periodically.

Software development lifecycle. Khan Academy maintains documented software development lifecycle policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. We follow NIST and OWASP best practices and recommendations in the course of our product development.

Administrative Safeguards

Risk management. Khan Academy employs a cross-functional risk management process to identify and manage strategic, operational and compliance risks. A variety of methods are used to assess and manage risk, including policies, procedures, and use of industry standard tools to monitor and protect data and systems.

Background checks. Khan Academy employees are screened with background checks prior to their employment with us.

Employee use of equipment and tools. Laptops issued to our employees for work purposes are managed to ensure that they are properly configured, regularly updated, and tracked. Our default configuration includes full-disk encryption of hard drives, on-device threat detection and reporting capabilities, and lock when idle for a specified amount of time. All laptops are securely wiped following NIST guidelines before we re-issue or dispose of them. All employees are required to use multi-factor authentication and strong passwords following NIST guidelines to access Khan Academy resources.

Vulnerability management. Khan Academy uses a variety of tools, practices and procedures to monitor and protect our data and systems. Khan Academy maintains a confidential vulnerability disclosure program that fields reports from security researchers, and reports are promptly triaged, prioritized and addressed according to their severity.

Physical security.

Access to Khan Academy's headquarters office is restricted to authorized personnel and visitors. All external entrances are locked and require badge access.

Employee Training

wnyric
www.wnyric.org
Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892
erie boces

Our employees are required to complete information security awareness training upon hire and periodically thereafter. Employees that have access to Student Education Records receive training on applicable federal and state privacy laws. Personnel are required to acknowledge and agree to our written information security policy and our employee handbook which, among other things, highlights our commitment to keep Student Education Records and confidential information secure.

Third party service providers; Vendor management

In order to provide its services, Khan Academy may engage third parties to provide services such as server and data hosting, email delivery, customer service support, analytics and communication tools and services. We review third party service provider security controls, privacy and data protection policies, and contract terms upon initial engagement and periodically thereafter. Third party service providers are required to enter into written agreements whereby they agree to protect the security, privacy and confidentiality of personally identifiable information shared in the context of the services relationship. Third party service providers are prohibited from engaging in targeting advertising and any other use of Student Education Records except in support of the services we provide to the customer.

Incident management

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents.

Khan Academy's incident response procedures include procedures to provide prompt notification regarding security incidents as required by applicable laws, including a description of the security incident based on available information, and contact information for the Khan Academy representative(s) who will be available to assist the subscribing school district.

Khan Academy may review and update this Data Security and Privacy Plan from time to time, provided that any such updates shall not materially diminish the overall security of the Service or Student Protected Data.

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the RFP" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor [*check one*] _____will __x__will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the RFP. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the RFP, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the RFP," below. For clarity, Khan Academy provides its services directly. In order to provide its services, Khan Academy engages third parties to provide certain support services, such as website application and data hosting, email delivery, customer service support, analytics and communication tools and services. Khan Academy does not consider such service providers to be subcontractors.

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

(f) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the RFP is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

Vendor may also dispose of accounts or personally identifiable information contained in accounts when no longer needed for the purpose for which it was obtained or as required by applicable law. Methods of disposition include erasing any Personally identifiable information contained in Student Data or permanently encrypting or otherwise modifying the Personally identifiable information contained in Student data to make it unreadable or indecipherable, de-identified or anonymized. The duty to dispose of Student Data shall not extend to data that has been rendered unreadable or indecipherable, de-identified or anonymized.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the RFP and the terms of this DSA.

(a) Limit internal access to Education Records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors or service providers that need access in order to assist Vendor in fulfilling one or more of its obligations under the RFP.

(c) Not use Education Records for any purposes other than those explicitly authorized in this DSA. Such purposes include providing the Service and related purposes described in the Agreement, including fulfilling requests made by a Participating Educational Agency and as otherwise directed or approved by the relevant Participating Educational Agency.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the RFP or as otherwise expressly permitted under the Agreement, unless:

(i) the parent or eligible student has provided prior written consent;
(ii) the disclosure is by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
(iii) as directed or permitted by Participating Educational Agency or this DSA, including as authorized under statutes referred to herein;
(iv) to authorized users of the Service, including students and their parents; or
(v) as permitted by law, to protect the safety or integrity of users or others, or the security of the Service

This prohibition against disclosure shall not apply to De-Identified Data, information disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Vendor pursuant to this DSA.

For clarity, Vendor may use education records for purposes of providing the Service, as set forth in the MLSA and the TOS, subject to compliance with this DSA

Vendor will use Student Data in order to provide access to and use of Vendor's Services as set forth the MLSA including (i) to provide Students with individual Website accounts; (ii) to provide adaptive and/or customized student learning features of the Service and educational programs offered through the Service; (iii) to allow School Personnel, and Parents and coaches associated with Students, to review and evaluate Student educational achievement and progress on the Service; (iv) to communicate with users regarding use of the Service and provide information regarding educational and enrichment programs; and (v) as otherwise required or permitted by applicable law.

Permitted use of data includes sending in-app or emailed communications relating to the Services, including prompts, messages and content relating to the use of the Services, for example; onboarding and orientation communications, prompts for Students to complete, or teachers to assign exercises or provide feedback as part of the learning exercise, periodic activity reports, suggestions for additional learning activities in the Services, service updates (for example new features or content, and information about special or additional programs offered through the Services or website/application).

Certain programs may be offered only with the approval of Erie 1 BOCES, the Participating Educational Agency or the Parent, in accordance with applicable laws. The Agreement does not restrict Vendor programs or activities authorized by the Parent or legal guardian.

Permitted disclosures shall include disclosure of protected data to Vendor's employees, agents, third party service providers and program partners that have a legitimate need to access such information in order to provide their services to Vendor, and as permitted by the functionality of the service.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the RFP," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Addendum) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law.

(h) Upon request, promptly pay for or reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full actual and reasonable cost of notification, to the extent that they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees provided, however, such incident is not attributed to Erie 1 BOCES, another BOCES, or a Participating School District's use of the Service or otherwise a result of the Participating Educational Agency's actions or inactions.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES if it determines that there has been any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

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

(b) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(c) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will use reasonable efforts to promptly inform Michelle Okal-Frink or her designees.

DocuSign Envelope ID: DC4A89E5-D55F-4977-BF19-5AC1F06177FB



(d) Vendor will use reasonable efforts to consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

(e) This Section 6 shall not restrict Vendor's ability to provide separate breach notification to its customers, including parents and other individuals with Website accounts.

(f) In the event of a breach originating from Erie 1 BOCES or Participating Educational Agency's use of the Service, Erie 1 BOCES or Participating Educational Agency shall cooperate with Vendor to the extent necessary to expeditiously secure the impacted data.

DocuSign Envelope ID: DC4A89E5-D55F-4977-BF19-5AC1F06177FB



**EXHIBIT D (CONTINUED)**

ERIE 1 BOCES

## PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at http://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/data-privacy-security/report-improper-disclosure.

**BY THE VENDOR:**

DocuSigned by:
Jason Hovey
77B08E305C4E491...

**Signature**

Jason Hovey

**Printed Name**

Director School Partnerships

**Title**

6/10/2024

**Date**

DocuSign Envelope ID: DC4A89E5-D55F-4977-BF19-5AC1F06177FB

DocuSign Envelope ID: DC4A89E5-D55F-4977-BF19-5AC1F06177FB



## EXHIBIT D (CONTINUED)

In accordance with Education Law §2-d(3)(c) and Section 121.3 of the implementing Regulations, set forth below is the "Supplemental Information" required to be posted on the Participating Educational Agency's website.

**Supplemental Information**
to
**Parents Bill of Rights**

Erie 1 BOCES has entered into an RFP with Khan Academy, Inc. which governs the availability to Participating Educational Agencies of the following Product(s): Khan Academy Free Version

Pursuant to and as fully described in the RFP, Vendor will provide access to and use of the Khan Academy website, mobile application and related services (collectively, the "Services") to Participating Educational Agencies (and their students and school personnel) for educational activities under the direction of the Participating Educational Agency.

Services provided under this Agreement are limited to free use of the website and under the Vendor Terms of Service posted on the website (www.khanacademy.org) and support services specifically included in the RFP.

**Khan Academy Standard Features**. Khan Academy provides access to a website located at http://khanacademy.org and related mobile applications (collectively "Website"), through which it provides free educational services, including, but not limited to, educational content, and to other products and services that Khan Academy may provide now or in the future (collectively, the "Service"). The Service is governed by and further described in Khan Academy's Terms of Service and Privacy Policy.

Pursuant to the RFP response, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

**Exclusive Purpose for which Protected Data will be Used**: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the Services under the RFP. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the RFP or as otherwise legally permissible. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be Sold, or released or used for any commercial or marketing purposes.

**Oversight of Subcontractors**: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the RFP (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation to comply with data security and privacy standards no less restrictive than those required of Vendor under the MLSA, this DSA, and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements, as follows:

Khan Academy maintains a vendor management program to vet and manage third party service providers that have access to protected data in the course of providing services to Khan Academy. Khan Academy reviews third party service provider security controls, privacy and data protection policies, and contract terms upon initial engagement and periodically thereafter. Third party service providers are required to agree in writing to protect the security, privacy and confidentiality of personally identifiable information shared in the context of the services relationship consistent with Khan Academy's obligations to its customer.

**Duration of the RFP and Protected Data Upon Expiration:**

The RFP commences on July 1, 2024 and expires on June 30, 2027, unless earlier terminated by the parties.

Upon expiration of the RFP without renewal, or upon termination of the RFP prior to expiration, user accounts created pursuant to the Service will remain open and available for use unless and until the Participating Educational Agency or its personnel instructs Vendor to delete the accounts, or the teacher, Parent or Student takes action to delete the account.

Upon request from the Participating Educational Agency to delete School Accounts, Vendor will securely delete, destroy or permanently De-Identify any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data.

Prior to terminating School Accounts (and associated Protected Data) at the direction of the Participating Educational Agency or its personnel, Vendor may (but is not required to) invite Students or Parents to establish a personal account for purposes of retaining any content generated or provided by the Student (including the Student's learning activity on the website). Personally identifiable information required to establish the account and maintain the content (for example, username, password, age, and the user's learning activity) will be retained. Any such personal accounts will be established under Vendor's standard account opening process, including by obtaining Parent consent where required by applicable law.

Upon termination of the Services, Vendor will not be obligated to export Protected Data back to the Participating Educational Agency. Personally identifiable information that is not retained in a personal account as provided herein will be disposed of rather than returned to the Participating Educational Agency.

Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data from any deleted account, on any storage medium whatsoever. Upon request, Vendor or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

**Challenging Accuracy of Protected Data:** Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Student Data held by Vendor is accessible in the Student's account profile, and may be viewed by the Student or Parent at any time in the Student's account. Parents may elect to open a free Parent account associated with their Student's account on the Website, and will be able to view and correct

the Student's account profile information and view their account activity through the Parent account. Certain account controls, including the ability to modify the account profile or delete the account, may be exercisable by the teacher that created the account, by the student account holder or their parent with an associated account. Data that is accessible in the account is limited to basic account data (such as username, password, birthdate) and information regarding Khan Academy usage data (such as videos watched and exercises completed); it does not include school data such as test scores, grades or attendance records.

If Vendor receives a request from a Parent requesting correction of Student data collected by Vendor or its subcontractors, Vendor will either (i) directly assist the Parent or guardian with respect to their request to correct Student data held by Vendor, (ii) direct their request to the Student's teacher or Participating Educational Agency for resolution by the School or (iii) request that the Parent direct their request to the Student's teacher or School for resolution by the Participating Educational Agency.

**Data Storage and Security Protections:** Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

**Encryption of Protected Data**: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5. The Khan Academy website is hosted on the Google Cloud Platform (GCP). All data on GCP is encrypted at rest in accordance with Google's security practices.