



Kenton County School District | It's about ALL kids.

Issue Paper

ENC.

DATE:

August 17, 2026

AGENDA ITEM (ACTION ITEM):

Consider/Approve the vendor assurance and terms and conditions between Knowt and Snorkl and the Kenton County School District.

APPLICABLE BOARD POLICY:

01.1 - Legal Status of the Board

HISTORY/BACKGROUND:

Knowt and Snorkl are AI tools that supplement the use of MagicSchool by providing functions that are not available through MagicSchool at this time. With Knowt, students and teachers can upload notes or resources related to what they are learning. Knowt then provides an interactive study platform that allows students to use digital flashcards and practice tests generated from the specific sources uploaded. Teachers can see student progress on the activities and get insights on student learning through the embedded analytics. Snorkl provides students with a digital whiteboard where students can draw, type and record their written or verbal responses to a question or prompt, explaining their thinking. They will then receive instant AI feedback on their submitted responses and reasoning to continue to support their learning. Teachers have access to all student responses as well as insights through the teacher dashboard that identify areas of strength and need, as well as in identifying common misconceptions and errors that need to be addressed.

FISCAL/BUDGETARY IMPACT:

No budgetary impact

RECOMMENDATION:

Approve the vendor assurance and terms and conditions between Knowt and Snorkl and the Kenton County School District.

CONTACT PERSON:

Jena Smiddy

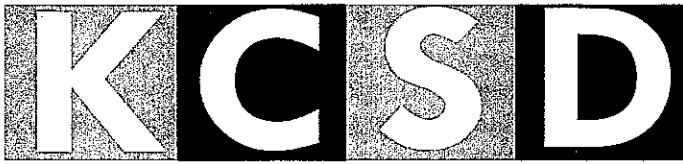
Principal/Administrator

District Administrator

Superintendent

Use this form to submit your request to the Superintendent for items to be added to the Board Meeting Agenda.

Principal—complete, print, sign and send to your Director. Director—if approved, sign and put in the Superintendent's mailbox.



Kenton County School District | It's about ALL kids

THE KENTON COUNTY BOARD OF EDUCATION

1055 EATON DRIVE, FORT WRIGHT, KENTUCKY 41017

TELEPHONE: (859) 344-8888 / FAX: (859) 344-1531

WEBSITE: www.kenton.kyschools.us

Dr. Henry Webb, Superintendent of Schools

**VENDOR ASSURANCES REGARDING PROTECTION OF
PERSONAL AND CONFIDENTIAL INFORMATION**

Data Security and Breach Protocols

Vendors that receive Personal Information from Kenton County Board of Education (herein referred to as "KCBOE") as defined by and in accordance with Kentucky's Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq., (the "Act"), shall secure and protect the Personal Information by, without limitation, complying with all requirements applicable to non-affiliated third parties set forth in the Act.

"Personal Information" is defined in accordance with KRS 61.931(6) as "an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

- a) An account number, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
- b) A Social Security number;
- c) A taxpayer identification number that incorporates a Social Security number;
- d) A driver's license number, state identification card number or other individual identification number issued by any agency as defined under the Act;
- e) A passport number or other identification number issued by the United States government; or
- f) Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by the Family Education Rights and Privacy Act, as amended 20 U.S.C. sec 1232g."

As provided in KRS 61.931(5), a "non-affiliated third party" includes any person or entity that has a contract or agreement with the KCBOE and receives (accesses, collects or maintains) personal information from the KCBOE pursuant to the contract or agreement.

The vendor hereby agrees to cooperate with the KCBOE in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

The vendor shall notify as soon as possible, but not to exceed seventy-two (72) hours, KCBOE, the Commissioner of the Kentucky State Police, the Kentucky Auditor of Public Accounts, the Commonwealth (Kentucky) Office of Technology, and the Commissioner of the Kentucky Department of Education of a determination of or knowledge of a breach, unless the exception set forth in KRS 61.932(2)(b)(2) applies and the vendor abides by the requirements set forth in that exception. Notification shall be in writing on a form developed by the Commonwealth (Kentucky) Office of Technology.

The vendor hereby agrees to report to the KCBOE, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site.

The vendor hereby agrees that the KCBOE may withhold payment(s) owed to the vendor for any violation of the Act's notification requirements.

The vendor hereby agrees to undertake a prompt and reasonable investigation of any security breach as defined under the Act in accordance with KRS 61.933.

Upon conclusion of an investigation of a security breach as defined under the Act as required by KRS 61.933, the vendor hereby agrees to an apportionment of the costs of the notification, investigation, and mitigation of the security breach.

In accordance with KRS 61.932(2)(a), the vendor shall implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent as the security and breach investigation procedures and practices established by the Commonwealth (Kentucky) Office of Technology and that are reasonably designed to protect the Personal Information from unauthorized access, use, modification, disclosure, manipulation, or destruction.

Student Data Security

Pursuant to KRS 365.734, if the vendor is a cloud computing service provider (which is defined pursuant to KRS 365.734(1)(b) as any person or entity other than an educational institution that operates cloud computing services) or, through service to the KCBOE, becomes the equivalent of a cloud computing service provider, the vendor further hereby agrees that:

- The vendor shall not process student data as defined pursuant to KRS 365.734 for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the vendor receives express permission from the student's parent. The vendor shall work with the KCBOE to determine the best method of collecting parental permission.
- With a written agreement for educational research, the vendor may assist the KCBOE to conduct educational research as permitted by the Family Education Rights and Privacy Act of 1974, as amended, 20 U.S.C. sec. 1232g.
- Pursuant to KRS 365.734, the vendor shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.
- Pursuant to KRS 365.734, the vendor shall not sell, disclose, or otherwise process student data for any commercial purpose.
- Pursuant to KRS 365.734, the vendor shall certify in writing to the agency that it will comply with KRS 365.734(2).

Family Educational Rights and Privacy Act, National School Lunch Act and Child Nutrition Act

If during the course of this agreement, the KCBOE discloses to the vendor any data protected by the Family Educational Rights and Privacy Act of 1974 (FERPA), as amended (20 U.S.C. sec. 1232g, *et seq.*), and its regulations, and data protected by the Richard B. Russell National School Lunch Act (NSLA) (42 U.S.C. sec. 1751 *et seq.*, and the Child Nutrition Act of 1966 (CNA) (42 U.S.C. sec. 1771 *et seq.*), the vendor agrees that it is bound by and will comply with the confidentiality, security and redisclosure requirements and restrictions stated in FERPA, NSLA and CNA.

The vendor hereby agrees to report to the KCBOE, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site.

The vendor agrees that FERPA-protected information is confidential information. FERPA-protected information includes, but is not limited to the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and other information that, alone or in combination, is linked or linkable to a specific

student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

The vendor understands and acknowledges that any unauthorized disclosure of confidential information is illegal as provided in FERPA and in the implementing federal regulations found in 34 CFR, Part 99. The penalty for unlawful disclosure is a fine of not more than \$250,000 (under 18 U.S.C. sec. 3571) or imprisonment for not more than five years (under 18 U.S.C. sec. 3559), or both.

The vendor understands and acknowledges that children's free and reduced price meal and free milk eligibility information or information from the family's application for eligibility, obtained under provisions of the NSLA or the CNA is confidential information and that any unauthorized disclosure of confidential free and reduced price lunch information or information from an application for this benefit is illegal. The penalty for unlawful disclosure is a fine of not more than \$1,000.00 (under 7 C.F.R. 245.6) or imprisonment for up to one year (under 7 C.F.R. 245.6), or both.

In the event there is a conflict between this agreement and any other agreement between KCBOE and Vendor, the terms of this agreement shall apply.

Knowt Inc.

Vendor Name

16192 Coastal Hwy, Lewes, DE, 19958

Vendor Address

646-661-9118

Vendor Telephone

schools@knowt.com

Vendor Email Address



Signature by Vendor's Authorized Representative

Abheek Pandoh

Print Name

5/12/26

Date

KNOWT, INC. ("SERVICE PROVIDER") STUDENT DATA PROCESSING ADDENDUM ("DPA")

Effective Date: 9/23/2024

This DPA is incorporated into our Terms of Service (the "Agreement") between your School named in your sign-up ("School") and Knowt, Inc. ("Knowt"). The DPA applies to all Processing of Student Personal Data by Knowt under the Agreement. Should there be a conflict between this DPA and the Agreement, this DPA will govern. This DPA is effective when you click to accept it. If you are accepting on behalf of School, you represent and warrant that (i) you have full legal authority to bind the School to this DPA; (ii) you have read and understand this DPA; and (iii) you agree, on behalf of the School, to this DPA. If you signed an offline variant of the Agreement or the DPA for use of Knowt, the terms below do not apply to you and your offline terms govern your use of the Knowt.

1. **Definitions.** In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:
 1. **"Applicable Laws"** means all statutes, laws, rules, regulations, ordinances, and the like of any federal, international, city, state, provincial, or local government or governmental agency applicable to Services under the Agreement including without limitation Data Protection Laws.
 2. **"Confidential Information"** is defined in the Agreement.
 3. **"Data Breach"** means unauthorized acquisition of, access to, disclosure of, or use of, Student Personal Data.
 4. **"Data Protection Laws"** means Applicable Laws relating to privacy, security, or protection of Personal Data, as may be defined by such laws, including, for example and to the extent applicable, but not limited to: the Federal Education Privacy Rights Act ("FERPA"), the Children's Online Privacy Protection Act ("COPPA"), the New York State Education Law 2-D Section, the California Consumer Protection Act ("CCPA"), the EU General Data Protection Regulation (Regulation 2016/679) ("GDPR"), regulations and official guidance adopted thereunder, and any subsequent supplements, amendments, or replacements to the same.
 5. **"Data Subject"** means data that relates to an identified or identifiable natural person or as otherwise defined under Data Protection Laws.
 6. **"Education Records"** are records, files, documents, and other materials directly related to a Student and maintained by the School and/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.
 7. **"Process, processed, or processing"** means the collection, receipt, recording, organization, structuring alteration, use, transmission, access, sharing, provision, disclosure, distribution, copying, transfer, storage, management, retention, deletion, combination, restriction, summarizing, aggregation, correlation, inferring, derivation, analysis, adaptation, retrieval, consultation, destruction, disposal, or other handling of Personal Data.

8. **"School Official"** means, for the purposes of this DPA and pursuant to 34 CFR Section 99.31(b), a contractor that: (1) performs an institutional service or function for which the School, local education agency or institution would otherwise use employees; (2) is under the direct control of the School, local education agency or institution with respect to the use and maintenance of Student Personal Data including Education Records, and (3) is subject to 34 CFR Section 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.
9. **"Sell" or "selling"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Data to another business or a third party for monetary or other valuable consideration, or as otherwise defined under applicable law.
10. **"Services"** means services provided by Knowt under the Agreement and all schedules, order forms, and statements of work thereunder.
11. **"Share" or "sharing"** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for cross-context behavioral advertising (as that term is defined in the CCPA), whether or not for monetary or other valuable consideration.
12. **"Student Personal Data"** any data whether gathered by Knowt or provided by the School, its students, teachers or other educators, or students' parents or legal guardians that Knowt accesses in the course of providing the Services under the Agreement that is descriptive of the student including, but not limited to information in the student's Education 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 Personal Data includes device identifiers and information and usage data. Student Personal 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 Personal 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 A is confirmed to be collected or processed by Knowt pursuant to the Services. Student Personal Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Knowt's services.
13. **"Sub-processor"** means any person or entity engaged by Knowt that processes Student Personal Data.
14. The terms **"Controller," "Processor," "Data Processor,"** and **"Service Provider"** shall have the same meaning as in Data Protection Laws.

2. **Notices.** All notices or communications required or permitted hereunder may be given via email to the representative email address used to register for an account on behalf of the school, or where Knowt is to receive notice to schools@knowt.com.

3. **Data Ownership/Licenses**

3.1. **Ownership.** For purposes of this DPA, as between the parties, School retains all right, title, and interest in Student Personal Data.

3.2. **License.** Subject to its compliance with the Agreement and DPA, School grants to Knowt worldwide, perpetual, fully paid-up right and license under all applicable intellectual property laws to make, use, copy, distribute, display, organize, create derivative works from, and otherwise Process, the Student Personal Data, and to sublicense all the foregoing rights to Sub-processors, as necessary for the Services, rights, and obligations under the Agreement and this DPA.

4. **Scope of Processing**

4.1. **Roles of Parties.** The parties acknowledge and agree that with respect to processing of Student Personal Data, Knowt is a Processor and a service provider (as that term is defined in Data Protection Laws) and School is a Controller (or Business, if applicable), except that if School is a Processor in which case Service Knowt is a Sub-processor. If School is a Processor of Student Personal Data, School represents and warrants that School's instructions and Processing of Student Personal Data, including its appointment of Knowt as a Sub-processor, have been authorized by the respective Controller.

4.2. **Details of Processing.** Exhibit A to this DPA provides information about the subject matter and details of the Processing of Personal Data.

5. **Parent Access.** To the extent required by applicable data protection law, the School shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Personal Data and education records, correct erroneous information, procedures (if applicable law requires) to export, and procedures to delete Student Personal Data, consistent with the functionality of the Services. Knowt shall respond in a reasonably timely manner (and no later than thirty (30) days from the date of the request, or as pursuant to the time frame required by applicable data protection law, whichever is sooner) to a School's request for access, correction, deletion, or export of Student Personal Data. If a parent, legal guardian, or other individual contacts Knowt to access, correct, delete, or export Student Personal Data accessed pursuant to the Services, Knowt shall refer the parent or individual to the School, who will follow the necessary and proper procedures regarding the requested information.

6. **Law Enforcement Requests.** If law enforcement or other government entities ("Requesting Party(ies)") contact Knowt with a request regarding Student Personal data held by Knowt pursuant to the Services, Knowt shall notify the School in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the School of the request.

7. **Subprocessors.**

7.1. **Approved Sub-Processors.** The School authorizes access or transfer to Knowt's Sub-processors. At present, the Sub-processors Knowt uses are listed in Exhibit D. Knowt will provide ten (10) calendar days' notice before utilizing a new Sub-processor by posting an update to the list at knowt.com/privacy. The School authorizes Knowt to use any such Sub-

processor to process Student Personal Data unless School objects within ten (10) calendar days of such notification. Any such objection must be based on reasonable grounds that any such Sub-processor is unable to adequately protect the Student Personal Data in accordance with the Agreement. If such objection is justified, the School and Knowt will work together to find a mutually acceptable resolution to such objection, and if unsuccessful, the School's sole remedy is termination of the relevant Services under the terms of the Agreement.

7.2. Responsibility. Knowt shall enter into written agreements with all Subprocessors performing functions for Knowt in order for Knowt to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Personal Data in a manner substantially similar to this DPA.

8. Location of Processing. Knowt will only Process Student Personal Data in the countries and regions listed in Exhibit A ("Approved Regions"), or such other countries and regions as instructed or authorized by the School (where the School's instruction or authorization received by email or other electronic means is acceptable).

9. Cross-Border Data Transfers.

9.1. With regard to countries, regions, or territories with Data Protection Laws requiring a mechanism for valid export of Student Personal Data (such countries, regions, or territories, are "Limited Transfer Region(s)" and such data is "Limited Transfer Data"), Knowt may not transfer, export, receive, or Process such Limited Transfer Data outside of such Limited Transfer Regions unless it or its Sub-processors take measures to adequately protect such data consistent with applicable Data Protection Laws. Such measures may include (to the extent consistent with Data Protection Laws):

- 9.1.1.** Processing Student Personal Data in a country, a territory, or one or more specified jurisdictions that are considered under Data Protection Laws as providing an adequate level of data protection);
- 9.1.2.** The parties' agreement to enter into and comply with the Standard Contractual Clauses in Exhibit E and any successors or amendments to such clauses or such other applicable contractual terms adopted and approved under Data Protection Laws;
- 9.1.3.** Processing in compliance with Binding Corporate Rules in accordance with Data Protection Laws;
- 9.1.4.** Implementing any other data transfer mechanisms or certifications approved under Data Protection Laws, including, as applicable, the Data Privacy Framework (and any approved successor or replacements thereto); or

9.2. To the extent that any substitute or additional appropriate safeguards or mechanisms under any Data Protection Laws of Limited Transfer Regions are required to transfer Student Personal Data from a Limited Transfer Region, as applicable, to any third country, the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this DPA governing the parties' Processing of Limited Transfer Data.

10. Duties of the School

- 10.1. Provide Parents COPPA Notice and Gain Consent.** Knowt provides schools with its COPPA notice to parents and a template consent form. Schools agree to provide this notice to parents or legal guardians of students under age (13) thirteen prior to enabling those students' use of the platform and at least annually, and to obtain parental consent through a method approved by the Federal Trade Commission or by using the template consent form to gain parents' physical signature. Upon request, School must provide Knowt evidence or documentation that it has provided parents' notice and gained parent consent.
- 10.2. Provide Student Data in Compliance with Applicable Laws.** School shall provide Student Personal Data for the purposes of obtaining the Services in compliance with all applicable data protection laws, as well may be amended from time to time.
- 10.3. Annual Notification of Rights and FERPA.** If the School has a policy of disclosing Education Records and/or Student Personal Data under FERPA (34 CFR Section 99.31(a)(1)), the School 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. For the avoidance of doubt, to the extent Personally Identifiable Information, as defined by FERPA, is transmitted to Knowt, Knowt shall be considered a School Official with a legitimate educational interest, under the direct control of the School as it pertains to the use of Education records.
- 10.4. Reasonable Precautions.** School shall take reasonable precautions to secure usernames, passwords, and means of gaining access to the Services and hosted Student Personal Data.
- 10.5. Unauthorized Access Notification.** School shall notify Knowt promptly of any known unauthorized access. School will assist Knowt in any efforts by Knowt to investigate and respond to any unauthorized access.

11. Duties of Knowt/Processing Instructions

- 11.1. Privacy Compliance.** Knowt shall comply with all applicable Data Protection Laws.
- 11.2. Instructions.** Knowt will use, retain, and disclose Student Personal Data solely for the specific business or education purposes of providing the Services and in accordance with the School's instructions, which are set forth in the Agreement, DPA, and other agreements between the parties for the Services, or as otherwise permitted under applicable Data Protection Laws. Knowt will inform School if any of School's instructions infringes any applicable Data Protection Laws. For avoidance of doubt, Knowt is an interactive and social learning platform that allows Students to add notes, media, and content, use generative artificial intelligence to create flashcards and learning tools, and to share the notes, media, and content for, or access the notes, media, and content of, other students to use. Knowt will use, retain, and disclose Student Personal Data to facilitate these Services.
- 11.3. No Disclosure.** Knowt acknowledges and agrees that it shall not make any re-disclosure of Student Personal Data or any portion thereof, including without limitation, user content or other non-public information contained in the Student Personal Data other than as directed or permitted by the School or this DPA. This prohibition against disclosure shall not apply to summaries of de-identified information, Student Personal Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of Knowt pursuant to this DPA. Knowt will not Sell or Share Student Personal Data.

11.4. Knowt Employee Obligation. Knowt shall require its employees and agents with access to Student Personal Data to comply with all applicable provisions of this DPA with respect to the Student Personal Data shared under the Services Agreement. Knowt agrees that its employees and agents with access to Student Personal Data shall be subject to an appropriate confidentiality agreement.

11.5. De-Identified Data. School permits Knowt to deidentify or aggregate Student Personal Data in a manner that prevents individual identification of the School or Students. Knowt agrees not to attempt to re-identify de-identified Student Personal Data (except to the extent Knowt is testing its de-identification methods). De-identified data may be used by Knowt for the purposes allowed under FERPA and the following purposes: (1) assisting the School or other government agencies in conducting research and other studies; and (2) research and development of Knowt's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purposes and for customized student learning. Knowt's use of de-identified data shall survive the termination of this DPA or any request by the School to return or destroy Student Personal Data. Except for Subprocessors, Knowt agrees not to transfer de-identified Student Personal 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 School that has provided prior written consent for such transfer. Prior to publishing any document that names the School explicitly or indirectly, Knowt shall obtain the School's written approval of the manner in which de-identified data is presented.

11.6. Disposition of Data. Upon written request from the School, Knowt shall dispose of or provide a mechanism to transfer Student Personal Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the School is received, Knowt shall dispose of all Student Personal Data after providing the School with reasonable prior notice. The duty to dispose of Student Personal Data shall not extend to Student Personal Data that had been De-Identified or placed in a separate personal student account that was created by the student.

11.7. Advertising Limitations. Knowt is prohibited from using, disclosing, or selling Student Personal Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member, or group, for any purpose other than providing the Services. Knowt shall not disclose Student Personal Data for commercial purposes. This section does not prohibit Knowt from using Student Personal Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or School employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits. For the avoidance of doubt, Knowt may offer additional subscription upgrade options to Students where the marketing of those upgrades does not use Student Personal Data. If a Student or Student's parent or legal guardian chooses to purchase an upgrade, we or our Subprocessor may collect additional information, including payment information, to facilitate that student/parent or legal guardian request.

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

appropriate confidentiality agreement, Knowt will allow the School to audit the security and privacy measures that are in place to ensure protection of its Student Personal Data or any portion thereof as it pertains to the delivery of services to the School. Knowt will cooperate reasonably with the School and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of Knowt and/or delivery of Services to Students and/or School, and shall provide reasonable access to Knowt's facilities, staff, agents and School's Student Personal Data and all records pertaining to Knowt, School, and delivery of Services to the School. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

13. **Data Security.** Knowt agrees to utilize administrative, physical, and technical safeguards designed to protect Student Personal Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. Knowt shall adhere to any applicable law relating to data security. Knowt shall implement an adequate cybersecurity framework. Additionally, Knowt may choose to further detail its security programs and measures that augment or are in addition to the cybersecurity framework in Exhibit B. School may contact schools@knowt.com if there are any data security concerns or questions.
14. **Data Breach.** In the event of a Data Breach affecting Student Personal Data maintained by Knowt, Knowt shall notify the School without undue delay, and in any event within seventy-two (72) hours of confirmation of the incident, unless notification within this time would disrupt investigation of the incident by law enforcement. In such event, notification shall be made within a reasonable time after the incident. Knowt shall follow the following process:
 - 14.1. The security breach notification described above shall include, at a minimum, the following information to the extent known by Knowt and as it becomes available:
 - 14.1.1. The name and contact information of the reporting School subject to this section.
 - 14.1.2. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - 14.1.3. 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.
 - 14.1.4. 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
 - 14.1.5. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - 14.2. Knowt agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Personal Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - 14.3. Knowt 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 Personal Data or any portion thereof, including personally identifiable

information and agrees to provide School, upon request, with a summary of said written incident response plan.

14.4. School shall provide notice and facts surrounding the Data Breach to the affected Students, parents or legal guardians.

14.5. In the event of a breach originating from School's use of the Services, Knowt shall cooperate with School to the extent necessary to expeditiously secure Student Personal Data.

15. General Terms

15.1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

15.2. **Effect of Termination Survival.** If the Agreement is terminated, Knowt shall destroy all of School's Student Personal Data pursuant to Section 11.6 above.

15.3. **Priority of Agreements.** This DPA shall govern the treatment of Student Personal 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 Agreement, the terms of this DPA shall apply and take precedence. In the event of a conflict between the DPA and Exhibit C Supplemental State Terms, Exhibit C will control. Except as described in this paragraph herein, all other provisions of the Agreement shall remain in effect. In the event multiple teachers, educators, or administrators attempt to register for Knowt's services on behalf of a school, the first DPA will govern. Any other DPA or Agreement will be nullified.

15.4. **Entire Agreement.** This DPA and the 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.

15.5. **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.

15.6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE SCHOOL, 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 SCHOOL FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

- 15.7. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Knowt 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 Knowt sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, Knowt shall provide written notice to the School 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 Personal Data within the Agreement. The School has the authority to terminate the DPA if it disapproves of the successor to whom Knowt is selling, merging, or otherwise disposing of its business.
- 15.8. **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

SCHEDULE OF DATA

Category of Data

Device Identifiers and Information

Elements

IP addresses,

Use of cookies and similar technologies;

Device identifiers/mobile IDs

Operating systems, browsers

Software type, version, language, settings, configuration

Usage Data

Session start and end times;

Actions/clicks taken in service;

Access times and days;

Referring URLs

Length of time spent on different pages

Content and Files

Student and teachers' notes

Video or other content uploaded to the service

Practice exams or practice questions students provide

Instant messaging or posts and comments on posts

Communications

Students' email, chat, or other communication to Knowt

Demographics

Age/birthdate;

Gender

Parent/Guardian Contact Information

Parent first name and last name

Parent email address or other contact information

Student Name and Contact Information

First and last name;

Email address (school and/or personal)