

Profile Information

Student username and password

Profile picture;

Profile name;

Links to external social or other media profiles

Payment Information

Student or parent payment type;

Student or parent payment card number;

Payment card security number or pin;

Zip code/and or address associated with payment card

Class Information/Education Records

Students' grade level;

Classes in which student is enrolled;

Academic performance, e.g., exams on the Services

APPROVED REGIONS

United States

European Union

United Kingdom

EXHIBIT B
SECURITY MEASURES

Knowt's personnel will not process Student Personal Data without authorization. Personnel are obligated to maintain the confidentiality of any Student Personal Data and this obligation continues even after their engagement ends.

The technical and organizational measures implemented by Knowt to provide an appropriate level of security include:

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Measures for user identification and authorization

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure

EXHIBIT C
SUPPLEMENTAL STATE TERMS

To the extent applicable, the following terms will apply:

California

The Agreement, along with this DPA and any exhibits and appendices hereto, constitute the written agreement mandated by California AB 1584, codified at California Education Code § 49073.1, and includes the following statements:

- As set forth in section 4.1 of the DPA, Student Personal Data (including pupil records) continue to be the property of and under the control of the School;
- Student Personal Data collected pursuant to the Agreement, shall be used for no purpose other than those required or specifically permitted by the Agreement, this DPA, the instructions of the school, and the Knowt Privacy Policy;
- A parent, legal guardian, or eligible student may review personally identifiable information in the Student Personal Data that is collected by Knowt, and correct erroneous information;
- Knowt shall provide periodic security training designed to ensure the security and confidentiality of pupil records to those of its employees and staff who have access to Student Personal Data;
- Knowt shall notify the School in the event of a Data Breach, and to the extent required by Cal. Civ. Code § 1792.82 et seq, Knowt, in coordination with the School as appropriate, shall seek to notify the affected parent, legal guardian or eligible student;
- Student Personal Data shall not be retained or available to Knowt upon completion of the terms of the Agreement;
- Knowt and School, shall ensure compliance with the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g); and
- Knowt shall not use personally identifiable information to engage in targeted advertising.

Colorado

Knowt complies with all applicable requirements of Colorado's Student Data Transparency and Security Act, C.R.S. 22-16-101, et seq.

Connecticut

The Agreement, incorporating the DPA and any exhibits and appendices hereto constitute the written agreement mandated by the Connecticut Act Concerning Student Data Privacy, Conn. Gen. Stat. Ann. § 10-234aa-dd, and includes the following statements:

- As set forth in section 4.1 of the DPA, Student Personal Data, which includes student information, student records and student-generated content, are not the property of or under the control of Knowt;
- Section 11.6 of the DPA sets forth the means by which School may request the deletion of any Student Personal Data in the possession of the contractor that is not (A) otherwise prohibited from deletion or required to be retained under state or federal law, or (B) stored as a copy as part of a disaster recovery storage system and that is (i) inaccessible to the public, and (ii) unable to be used in the normal course of business by Knowt;

- Knowt shall not use Student Personal Data for any purposes other than those authorized pursuant to the Agreement, the DPA, any exhibits and appendices hereto, and the Knowt Privacy Policy;
- A student, parent or legal guardian of a student may review personally identifiable information contained in Student Personal Data collected by Knowt, and correct erroneous information, if any, in such student record;
- Knowt's core security commitments designed to ensure the security and confidentiality of Student Data are set forth in Exhibit B of this DPA;
- Knowt will notify the School when there has been a Data Breach affecting Student Personal Data;
- Student Personal Data shall not be retained or available to Knowt upon termination of the Agreement;
- Knowt and School, shall ensure compliance with the Family Educational Rights and Privacy Act of 1974, 20 USC 1232g, as amended from time to time;
- As set forth in section 15.6 of the DPA, the laws of the state of Connecticut shall govern the rights and duties of Knowt and the School; and
- As set forth in this DPA, if any provision of the Agreement or DPA or the application of the Agreement is held invalid by a court of competent jurisdiction, the invalidity does not affect other provisions or applications of the Agreement which can be given effect without the invalid provision or application.

Illinois

The Agreement, incorporating the DPA and any exhibits and appendices hereto constitute the written agreement mandated by the Illinois Student Online Personal Protection Act ("SOPPA"), codified at 105 ILCS 85/5, and includes the following statements:

- A listing of the categories or type of information to be provided to Knowt is available for public review the Knowt Privacy Policy;
- Pursuant to and as fully described in the Agreement, this DPA, and any exhibits and appendices hereto, Knowt has agreed to provide its flashcard study web and mobile app, features, and related services accessed through Knowt (collectively "Services") to the School;
- In performing its obligations under the Agreement, Knowt is acting as a school official with a legitimate educational interest; is performing an institutional service or function for which the School would otherwise use its own employees; is under the direct control of the School with respect to the use and maintenance of Student Personal Data; and is using Student Personal Data only for an authorized purpose and in furtherance of such legitimate educational interest;
- If a "Data Breach" is primarily attributable to Knowt, Knowt shall subject to any limitations in the Agreement, reimburse and indemnify School for any and all costs and expenses that the School incurs with: (a) providing notification to the parents of those students whose Student Personal Data was compromised and regulatory agencies or other entities as required by law or contract; (b) audit costs, fines, and any other fees or damages imposed against the School as a result of the security breach; and (c) providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws;
- The School shall notify Knowt when the Student Personal Data it has provided pursuant to the DPA is no longer needed for the School's purpose(s) under the Agreement and this DPA. If any of the Student Personal Data is no longer needed for purposes of the Agreement and this DPA, Knowt will delete or transfer Student Personal Data. Knowt will comply with School's request and

delete or transfer the Student Personal Data within a reasonable time period, not to exceed 30 days after verifying the written request, and according to a schedule and procedure as Knowt and the School may reasonably agree.

- Pursuant to SOPPA, School shall publish on its website a copy of the DPA, including this Appendix.

Kentucky

The Agreement, incorporating the DPA and any exhibits or appendices hereto constitute the written agreement mandated by Kentucky Revised Statutes 365.734, and includes the following statements:

- Knowt shall not process Student Data other than providing, improving, developing, or maintaining the integrity of the Services to the School as authorized pursuant to the Agreement. The Agreement, this DPA, any exhibits and appendices hereto, and the Knowt Privacy Policy set forth the exclusive purposes for which the Student Personal Data will be used by Knowt;
- Knowt shall not process Student Personal Data to advertise or facilitate advertising or to create or correct an individual or household for any advertisement purpose, and shall not sell, disclose or otherwise process Student Data for any commercial purpose.

Nevada

The Agreement, incorporating the DPA and any exhibits or appendices hereto constitute the written agreement mandated by Nevada Revised Statute 388.272, and includes the following statements:

- Knowt's commitments to protect the privacy and security of Student Personal Data are set forth in the DPA, including Exhibit B, and are outlined in the Knowt Privacy Policy; and
- Knowt acknowledges it may face potential liability as a penalty for intentional or grossly negligent noncompliance with this Agreement, subject to any limitations in the Agreement, including termination of the Agreement and payment of monetary damages, for any breach of the terms of this Agreement that cause actual harm to the School.

New York

The Agreement, incorporating the DPA and any exhibits or appendices hereto constitute the written agreement mandated by New York State Education Law § 2-d ("Section 2-d"), and Part 121 of the New York State Education Department ("NYSED") regulations implementing Section 2-d.

New York's Parents Bill of Rights for Data Privacy and Security is incorporated into the Agreement and Knowt agrees and acknowledges that:

- A student's personally identifiable information cannot be sold or released for any commercial purposes;
- Parents have the right to inspect and review the complete contents of their child's education record that is shared with or collected by Knowt;
- Knowt complies with all applicable state and federal laws that protect the confidentiality of personally identifiable information, and, as set forth Exhibit B of the DPA, employs safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, when data is stored or transferred;
- A complete list of all student data elements collected by Knowt is available for public review in the Knowt Privacy Policy; and
- Parents have the right to have complaints about possible breaches of student data addressed. Knowt will promptly address any such complaints directed to team@knowt.com

- The Agreement, the DPA, any exhibits or appendices hereto, and the Knowt Privacy Policy set forth the exclusive purposes for which the student data or teacher or principal data will be used by Knowt;
- Knowt may disclose the student data or teacher or principal data to subcontractors, or other authorized persons or entities ("Service Providers") in order to perform its duties under the Agreement. Knowt shall enter into written agreements with all Service Providers and shall be responsible for any actions of Service Providers that would be a breach of this document.
- Section 11.6 sets forth the time period, not to exceed 60 days, and process by which Knowt will either delete or transfer personally identifiable information upon the expiration of the contract or when requested to do so by notification from the contracting party;
- A parent, student, eligible student, teacher or principal may correct inaccurate student data or teacher or principal data that is collected by Knowt;
- Where required by applicable law, all student data or teacher or principal data will be stored within the United States and protected by employing administrative, physical, and technical safeguards designed to protect it from unauthorized access, disclosure, and use or acquisition by an unauthorized person, including when transmitting and storing such information.
- The data will be protected using encryption while in transit and at rest as further detailed in Exhibit B of the DPA.
- For purposes of compliance with NYSED regulation Part 121.6 implementing Section 2-d, details of Knowt's data privacy and security plan in Exhibit B.

North Carolina

The Agreement, incorporating the DPA and any exhibits or appendices hereto constitute the written agreement mandated by North Carolina General Statutes § 115C-402.5(b)(6), and includes the following statements:

- Knowt's commitments to safeguard the privacy and security of Student Personal Data are set forth in the DPA, including Exhibit B, and are outlined in the Knowt Privacy Policy; and
- Knowt acknowledges it may face potential liability as a penalty for intentional or grossly negligent noncompliance with this Agreement, including termination of the Agreement and payment of monetary damages, subject to any limitations in the Agreement, for any breach of the terms of this Agreement that cause actual harm to the School.

Oklahoma

The Agreement, incorporating the DPA and any exhibits or appendices hereto constitute the written agreement mandated by Oklahoma statute § 70-3-168, and includes the following statements:

- Knowt's commitments to safeguard the privacy and security of Student Personal Data are set forth in the DPA, including Exhibit B, and are outlined in the Knowt Privacy Policy; and
- Knowt acknowledges it may face potential liability as a penalty for intentional or grossly negligent noncompliance with this Agreement, subject to any limitations in the Agreement, including termination of the Agreement and payment of monetary damages for any breach of the terms of this Agreement that cause actual harm to the School.

Rhode Island

The Agreement, incorporating the DPA and any exhibits or appendices hereto constitute the written agreement mandated by Rhode Island HB 7124, as codified by General Laws § 16-104-1, and includes the following statements:

- Knowt shall process data of a student enrolled in kindergarten through twelfth (12th) grade ("Student Data") for the sole purpose of providing the Services to the School as authorized pursuant to the Agreement, this DPA, and any exhibits or appendices hereto. The Agreement, this DPA, and any exhibits or appendices hereto, and the Knowt Privacy Policy set forth the exclusive purposes for which the Student Personal Data will be used by Knowt;
- Knowt shall not process Student Personal Data for any commercial purposes, including, but not limited to, advertising purposes that benefit Knowt.

West Virginia

The Agreement, incorporating the DPA and any exhibits or appendices hereto constitute the written agreement mandated by West Virginia Code § 18-2-5h, and includes the following statements:

- Knowt's commitments to safeguard the privacy and security of Student Personal Data are set forth in this DPA, Exhibit B, and are outlined in the Knowt Privacy Policy; and
- Knowt acknowledges it may face potential liability as a penalty for intentional or grossly negligent noncompliance with this Agreement, including termination of the Agreement and payment of monetary damages, subject to any limitations in the Agreement, for any breach of the terms of this Agreement that cause actual harm to the School.

EXHIBIT D
SUB-PROCESSORS

This list identifies the Sub-processors authorized to Process Student Personal Data.

Company Name	Company location (location(s) of processing)	Services provided (description of subject matter, nature of Processing of Student Personal Data)	Duration of Processing of Student Personal Data
MixPanel	1 Front St, San Francisco, CA 94111	Site and App Analytics	e.g., until termination of Agreement or the School's request
Google (Analytics, Doubleclick)	1600 Amphitheatre Pkwy, Mountain View, CA 94043	Site and App Analytics, Advertising	e.g., until termination of Agreement or the School's request
Stripe	354 Oyster Point Blvd, South San Francisco, CA 94080	Payment processor	e.g., until termination of Agreement or the School's request
Publisher First, Inc., dba Freestar	20715 N Pima Rd Ste 108 Scottsdale, AZ 85255	Advertising	e.g., until termination of Agreement or the School's request
Vimeo	Video player vimeo.com , Inc. Attention: Data Protection Officer 330 West 34th Street, 10th Floor New York, New York 10001	Video player	e.g., until termination of Agreement or the School's request
Criteo	DPO-CRITEO 32 Rue Blanche 75009 Paris France	Advertising	e.g., until termination of Agreement or the School's request

EXHIBIT E
STANDARD CONTRACTUAL CLAUSES

- 1. EEA Personal Data Transfers.** Limited Transfer Data subject to the GDPR that the School transfers to Knowt will be governed by Module Two ("Controller to Processor") and Module Three ("Processor to Processor") of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as issued by the European Commission on June 4, 2021, and as also adopted by the Swiss Federal Data Protection and Information Commissioner ("FDPIC") (collectively "EU SCCs"), as applicable and as described herein. The elections and information required for the purposes of the EU SCCs is provided in Section 5 below and in Exhibit A to the DPA. The Parties agree that the EU SCCs are incorporated into this DPA without further need for reference, incorporation, or attachment and that by executing the DPA, each party is deemed to have executed the EU SCCs.
- 2. Swiss Personal Data Transfers.** Limited Transfer Data subject to the Swiss Federal Data Protection Act ("Swiss DPA") that the School transfers to Knowt will be governed by the EU SCCs with the following modifications:

 - 2.1.** References to "Regulation (EU) 2016/679" and any articles therefrom shall be interpreted to include references to the Swiss DPA.
 - 2.2.** References to "EU," "Union" and "Member State" shall be interpreted to include references to "Switzerland."
- 3. UK Personal Data Transfers.** Limited Transfer Data subject to the UK GDPR and UK Data Protection Act 2018 that the School transfers to Knowt will be governed by the EU SCCs and UK Transfer Addendum Version B1.0 (in force 21 March 2022) adopted by the UK Information Commissioner's Office (the "UK Transfer Addendum"). The Parties agree as follows:

 - 3.1.** Each Party agrees to be bound by the terms and conditions set out in the UK Transfer Addendum, in exchange for the other Party also agreeing to be bound by the UK Transfer Addendum.
 - 3.2.** The EU SCCs will be interpreted in accordance with Part 2 of the UK Transfer Addendum.
 - 3.3.** Sections 9 to 11 of the UK Transfer Addendum override Clause 5 (Hierarchy) of the EU SCCs.
 - 3.4.** For the purposes of Section 12 of the UK Transfer Addendum, the EU SCCs will be amended in accordance with Section 15 of the UK Transfer Addendum.
 - 3.5.** Information required by Part 1 of the UK Transfer Addendum is provided as Exhibit A to the

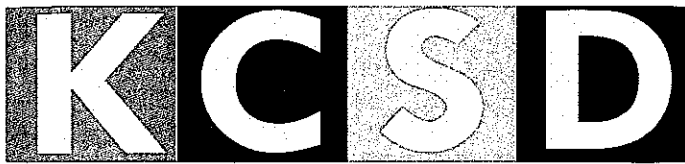
DPA.

- 3.6. To the extent that any revised transfer addendums or mechanisms are issued by the UK ICO, the Parties agree to incorporate such revisions in accordance with Section 18-20 of the UK Transfer Addendum.
- 3.7. The Parties agree that the UK Transfer Addendum is incorporated into this DPA without further need for reference, incorporation, or attachment and that by executing the DPA, each party is deemed to have executed the UK Transfer Addendum.
4. Other Limited Transfer Region Transfers. Limited Transfer Data that is not subject to the GDPR, Swiss DPA, or UK Data Protection Law, and that the School transfers to Knowt, will be governed by the EU SCCs with the following modifications: references to the General Data Protection Regulation will be replaced by applicable Data Protection Laws of the respective Limited Transfer Regions and for Clause 13 references to EU Member State shall be replaced with the applicable Limited Transfer Region.
5. EU SCC and UK Transfer Addendum Information.

SCC Clause	GDPR	Swiss DPA	UK Data Protection Law
Module in Operation Module Two (Controller to Processor) and Module Three (Processor to Processor)			
Clause 7- Docking Clause	(a) An entity that is not a party to these clauses may, with the agreement of the parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A. (c) The acceding entity shall have no rights or obligations arising under these		
Clause 9(a)- Use of Sub-processors	GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.		
Clause 11 (Redress)	Optional language in Clause 11 shall not apply.		

Clause 17- Governing Law	These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.	These Clauses shall be governed by the law of Switzerland, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.	These Clauses shall be governed by the law of the United Kingdom, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of England and Wales.
Clause 18 – Choice of Forum and Jurisdiction	The parties agree that those shall be the courts of Ireland.	The parties agree that those shall be the competent courts of Switzerland.	The parties agree that those shall be the competent courts of England and Wales.
Appendix, Annex I.A- List of Parties	The name, address, and contact person's name, position, and contact details, and each party's role in Processing Personal Data are as set forth in the DPA and Exhibit A to the DPA to which this Exhibit E is attached.		
Annex I>B – Description of Transfer	This information can be found in Exhibit A to the DPA to which this Exhibit E is attached. To the extent applicable, the descriptions of safeguards applied to the special categories of Personal Data can be found Exhibit B to the DPA to which this Exhibit E is attached.		
Clause 13 and Annex I>C – Competent Supervisory Authority	Identify the competent supervisory authority/ies in accordance with Clause 13: The Irish Data Protection Commission	Identify the competent supervisory authority/ies in accordance with Clause 13: FDPIC	Identify the competent supervisory authority/ies in accordance with Clause 13: UK Information Commissioner
Annex II – Technical and Organizational Measures	The description of technical and organization measures designed to ensure the security of Personal Data is in Exhibit B to the DPA to which this Exhibit E is attached.		
Annex II – Technical and Organizational Measures – Subprocessors	The description of technical and organization measures designed to ensure the security of Personal Data are described more fully Exhibit B to the DPA to which this Exhibit E is attached.		

Annex III – List of Subprocessors	As described in Exhibit D to the DPA to which this Exhibit E is attached.	
Ending the UK Transfer Addendum when the Approved Addendum changes	N/A	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party



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