

**WOODFORD COUNTY BOARD OF EDUCATION  
AGENDA ITEM**

**ITEM #: VII G DATE:** December 16, 2024

**TOPIC/TITLE:** Approve Contracts

**PRESENTER:** Danny Adkins

**ORIGIN:**

- ☐ TOPIC PRESENTED FOR INFORMATION ONLY (No board action required.)
- ☐ ACTION REQUESTED AT THIS MEETING
- ☒ ITEM IS ON THE CONSENT AGENDA FOR APPROVAL
- ☐ ACTION REQUESTED AT FUTURE MEETING: (DATE)
- ☐ BOARD REVIEW REQUIRED BY

- ☐ STATE OR FEDERAL LAW OR REGULATION
- ☐ BOARD OF EDUCATION POLICY
- ☐ OTHER:

**PREVIOUS REVIEW, DISCUSSION OR ACTION:**

- ☒ NO PREVIOUS BOARD REVIEW, DISCUSSION OR ACTION
- ☐ PREVIOUS REVIEW OR ACTION

- ☐ DATE:
- ☐ ACTION:

**BACKGROUND INFORMATION:**

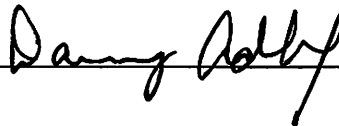
**SUMMARY OF MAJOR ELEMENTS:**

Attached Contracts: Data Sharing Agreement (Curriculum Associates); Data Sharing Agreement (Renaissance Learning); Fire Science Pathway MOU (City of Versailles); Metronet (Elevator Line); Safe Harbor Student Picture Agreement (Strawbringe).

**IMPACT ON RESOURCES:**

**TIMETABLE FOR FURTHER REVIEW OR ACTION:**

**SUPERINTENDENT'S RECOMMENDATION:** ☒ Recommended ☐ Not Recommended



**WOODFORD COUNTY BOARD OF EDUCATION  
AGENDA ITEM**

**ITEM #:**            **DATE:**

**TOPIC/TITLE:** Data Sharing Agreement

**PRESENTER:** Josh Rayburn

**ORIGIN:**

- ☐ TOPIC PRESENTED FOR INFORMATION ONLY (No board action required.)
- ☐ ACTION REQUESTED AT THIS MEETING
- ☒ ITEM IS ON THE CONSENT AGENDA FOR APPROVAL
- ☐ ACTION REQUESTED AT FUTURE MEETING:            (DATE)
- ☐ BOARD REVIEW REQUIRED BY

- ☐ STATE OR FEDERAL LAW OR REGULATION
- ☐ BOARD OF EDUCATION POLICY
- ☐ OTHER:

**PREVIOUS REVIEW, DISCUSSION OR ACTION:**

- ☐ NO PREVIOUS BOARD REVIEW, DISCUSSION OR ACTION
- ☐ PREVIOUS REVIEW OR ACTION

- ☐ DATE:
- ☐ ACTION:

**BACKGROUND INFORMATION:**

The board approves all contracts.

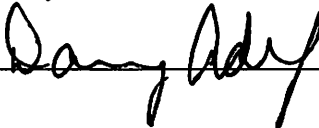
**SUMMARY OF MAJOR ELEMENTS:**

Data sharing agreements are agreements we use prior to sharing student data with a company. The board has a set data sharing agreement but if changes have to be made, the board must approve the amended changes.

**IMPACT ON RESOURCES:**

**TIMETABLE FOR FURTHER REVIEW OR ACTION:**

**SUPERINTENDENT'S RECOMMENDATION:** ☒ Recommended            ☐ Not Recommended





# WOODFORD COUNTY PUBLIC SCHOOLS

330 Pisgah Pike • Versailles, Kentucky 40383-9214 • (859) 879-4600

Danny Adkins, Superintendent

## *Memorandum of Agreement: Data Sharing Agreement*

### **Introduction**

- This document is an agreement between the Woodford County Public Schools (WCPS) and Curriculum Associates, **LLC Inc.** (hereinafter “the contracting party”) regarding the transfer of student and teacher data to the contracting party and the subsequent processing of that data.
- This agreement excludes any data which is freely and publicly available through other sources.
- Pursuant to KRS 61.932 and KRS 365.734, the parties to this agreement do hereby agree to the following:

### **Mechanism for Data Sharing**

WCPS and the contracting party will at the appropriate time agree on a file or data sharing process that will involve the transfer of the data via the public networks.

### **Obligations of the contracting party**

#### **The contracting party warrants that it will:**

- Use this data only for the joint project outlined above.
- Read and strictly comply with the provisions of the Family Educational Rights and Privacy Act (“FERPA”) and KFERPA; KRS 160.700 *et seq.* While in possession of this data maintain it in a secure, non-public location.
- Ensure that the student data will be accessed, used and manipulated **only** by those individuals necessary for the successful implementation of the project.
- Advise all individuals accessing the data on proper procedures for securely maintaining the data.
- Take appropriate technical and organizational measures against the unauthorized or unlawful accessing of the data.
- Securely delete all copies of the student data **upon written request** ~~when they are no longer required~~ **with the exception of backups, which will be automatically deleted over time in accordance with our data handling policy.** “Securely delete” means that industry standard methods will be taken for the purpose of ensuring that no unauthorized person shall be able to reasonably locate or extract the data after the deletion date.
- Promptly comply with any **written** request from WCPS to amend, transfer or delete the data or a subset thereof.
- The contracting party 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 purpose, and shall not sell, disclose, or otherwise process student data for any commercial purpose.
- Defend, indemnify, and hold harmless WCPS its agencies, officers and employees from any and all **third party** claims of any nature, including all **reasonable** costs, expenses, and **actual** attorney's fees, which may in any manner result from or arise out of this agreement, except for claims resulting from or arising out

of the WCPS' sole negligence. The legal defense provided by the contracting party to WCPS under this provision must be free of any conflicts of interest, even if retention of separate legal counsel for the WCPS is necessary. The contracting party also agrees to defend, indemnify, and hold WCPS harmless for all **reasonable** costs, expenses, and **actual** attorneys' fees finally awarded by a court or that are included in a settlement entered into by the parties. WCPS agrees to notify the contracting party of such a claim within a reasonable time and agrees to cooperate with the contracting party in the defense and any related settlement.

#### **Data Breach Act**

Pursuant to KRS 61.931, *et seq.*, the contracting party warrants it has procedures and practices in place to safeguard against security breaches.

In the event of a security breach, the contracting party shall notify the WCPS within 48 hours of the ~~suspected or~~ confirmed breach, and the contracting party shall begin conducting a reasonable and prompt investigation to determine whether the security breach has resulted in or is likely to result in the misuse of personal information.

Within 48 hours of completion of the investigation, the contracting party shall notify the above if the investigation finds that the misuse of personal information occurred or is likely to occur.

#### **Data Opt Out**

WCPS may provide a mechanism for students, parents or guardians to opt out of any data sharing agreement with any contracting party.

\_\_\_\_\_  
WCPS Superintendent

\_\_\_\_\_  
Contracting Party Representative

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date



## DSA for Curriculum Associates, LLC for your review

External

Inbox

Search for all messages with label Inbox

Remove label Inbox from this conversation



Tincher, Holly <holly.tincher@woodford.kyschools.us>

Wed, Nov 20, 8:07 AM (1 day ago)

to emily.vessels

Hi Emily -

Attached is a redlined copy of our standard DSA from Curriculum Associates, LLC for your review.

Thanks!

**Holly Tincher**

Systems Analyst

Woodford County Schools

859-879-4600 ext 2131





Vessels,  
Emily

9:45 AM (2 hours ago)

Holly, I am  
good with  
these  
proposed  
changes!  
Thanks!  
Emily H.  
Vessels

Associate  
Dinsmore &  
Shohl LLP •  
Legal  
Counsel  
101 South  
Fifth Street  
Suite 2500  
Louisvii

Hi Emily,

I am forwarding you the National Data Processing Agreement from Quizizz, Inc. for review. The privacy information on their website seems to indicate that this is compliant for Kentucky.

[privacy information from Quizizz](#)

Thank you,

**Holly Tincher**

Systems Analyst

Woodford County Schools

859-879-4600 ext 2131



One attachment • Scanned by Gmail



10:09 AM (3 hours ago)



**Vessels, Emily**

to me ☐

Hi Holly, apologies for the delay! This agreement looks acceptable as to form and legality.



**Emily H. Vessels**

Associate

Dinsmore & Shohl LLP • Legal Counsel

101 South Fifth Street

Suite 2500

Louisville, KY 40202

**T** (502) 540-2374 • **F** (502) 585-2207

**E** [Emily.Vessels@DINSMORE.COM](mailto:Emily.Vessels@DINSMORE.COM) • [dinsmore.com](http://dinsmore.com)

# **STANDARD STUDENT DATA PRIVACY AGREEMENT**

**(NDPA Standard Version 1.0/Vendor Modified etc.)**

**[INSERT SCHOOL DISTRICT OR LOCAL EDUCATION AGENCY]**

**and**

**[NAME OF PROVIDER]**

Quizizz

Copyright © 2020 Access 4 Learning (A4L) Community. All rights reserved.

This Student Data Privacy Agreement (“DPA”) is entered into on the date of full execution (the “Effective Date”) and is entered into by and between:

[School District Name], located at [Street, City, State] (the “Local Education Agency” or “LEA”) and  
[Provider Name], located at [Street, City, State] (the “Provider”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
  - ☒ If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
  - ☐ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit “H”. (Optional)**
  - ☐ If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “Services”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.



The designated representative for the LEA for this DPA is:

Name: \_\_\_\_\_ Title: \_\_\_\_\_

Address: \_\_\_\_\_

Phone: \_\_\_\_\_ Email: \_\_\_\_\_

The designated representative for the Provider for this DPA is:

Name: Daniella Piyavanich Title: Operations Lead

Address: 3110 Main Street, Building C, Santa Monica, CA, 90405

Phone: 818-253-1531 Email: daniella@quizizz.com

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

**LEA [School District Name]**

By: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

**[Insert Name of Provider] Quizizz Inc.**

By: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: Daniella Piyavanich Title/Position: Operations Lead

**STANDARD CLAUSES**

Version 1.0

**ARTICLE I: PURPOSE AND SCOPE**

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

**ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student 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 LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D".
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

## ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
    - i. The name and contact information of the reporting LEA subject to this section.
    - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
    - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
    - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
  - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
  - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

## ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service 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.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.



5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

**EXHIBIT "A"**  
**DESCRIPTION OF SERVICES**

Quizizz is a teacher-powered learning activity platform. Educators use Quizizz to create and deliver lessons, assignments, and formative assessments that motivate students to learn. Quizizz is used for all academic subject areas and supports students in all grade levels.

**EXHIBIT "B"**  
**SCHEDULE OF DATA**

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X

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

Category of Data	Elements	Check if Used by Your System
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

## **EXHIBIT "C"**

### **DEFINITIONS**

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

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

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

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

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

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

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

**School Official:** For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

**Service Agreement:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to,



information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

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

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

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

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

**EXHIBIT "D"**  
**DIRECTIVE FOR DISPOSITION OF DATA**

**[Insert Name of District or LEA]** Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

**1. Extent of Disposition**

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

**[Insert categories of data here]**

\_\_\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

**2. Nature of Disposition**

\_\_\_\_\_ Disposition shall be by destruction or deletion of data.

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

**[Insert or attach special instructions]**

**3. Schedule of Disposition**

Data shall be disposed of by the following date:

\_\_\_\_\_ As soon as commercially practicable.

\_\_\_\_\_ By **[Insert Date]**

**4. Signature**

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

**5. Verification of Disposition of Data**

\_\_\_\_\_  
Authorized Representative of Company

\_\_\_\_\_  
Date

**EXHIBIT "E"**  
**GENERAL OFFER OF PRIVACY TERMS**

**1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and [Insert Name of Originating LEA] ("Originating LEA") which is dated [Insert Date], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed Exhibit "E" to Provider at the following email address:

[NAME OF PROVIDER] Quizizz Inc.

BY: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the [Insert Name of Originating LEA] and the Provider. \*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. \*\*

[Insert Name of Subscribing LEA]

BY:

\_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

SCHOOL DISTRICT NAME: \_\_\_\_\_

DESIGNATED REPRESENTATIVE OF LEA:

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone Number: \_\_\_\_\_

Email: \_\_\_\_\_

## **EXHIBIT “F”**

### **DATA SECURITY REQUIREMENTS**

#### **Adequate Cybersecurity Frameworks** **2/24/2020**

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

#### Cybersecurity Frameworks

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

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

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

**EXHIBIT "G"**  
**Supplemental SDPC State Terms for [State]**  
Version \_\_\_\_\_

[The State Supplement is an *optional* set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (**Exhibit "H"** in this proposed structure).]

None

**EXHIBIT "H"**  
**Additional Terms or Modifications**  
Version \_\_\_\_\_

LEA and Provider agree to the following additional terms and modifications:

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

618-1/4715859.1

None



Student Data Privacy Addendum for Code.org

External

Data Sharing Agreements

Tincher, Holly

Oct 21, 2024, 10:49 AM

Hi Emily - Here is a link for a sample Student Data Privacy Addendum for Code.org for your review. Code.org DPA Thank you! Holly Tincher Systems Analyst Woodfor

Vessels, Emily

Oct 21, 2024, 2:58 PM

Holly, I am not able to access the link below. Can you send it via PDF? Emily H. Vessels Associate Dinsmore & Shohl LLP • Legal Counsel 101 South Fifth Street S

Tincher, Holly

Oct 21, 2024, 3:22 PM

Sorry Emily - Here is the downloaded document. Code.org sample-dpa.pdf

Vessels, Emily

Oct 22, 2024, 11:26 AM

Thanks! This privacy addendum is acceptable. Is there a service agreement that goes along with it? Code.org sample-dpa.pdf

Tincher, Holly

Oct 22, 2024, 2:01 PM

Hi Emily - This is not a service that we purchase, and do not see anything that looks like a Service Agreement on their Privacy Policy page. Does that make a di

Vessels, Emily

Oct 22, 2024, 3:26 PM

Interesting, it references a Service Agreement throughout the document. I was wondering mostly because of the termination provision in 6.2. If there is no Servi

Tincher, Holly

Oct 23, 2024, 8:48 AM

Is this it? Code.org Terms of Service

Vessels, Emily

Oct 23, 2024, 1:14 PM

I'm fine with the language in the terms of service and termination language within. Thanks! Is this it? Code.org Terms of Service

Tincher, Holly <holly.tincher@woodford.kyschools.us>

Oct 24, 2024, 9:50 AM

to Emily

My dear Emily

Dear

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

My dear Emily

## STUDENT DATA PRIVACY ADDENDUM<sup>1</sup>

This Student Data Privacy Addendum (“DPA”) is incorporated by reference into the Service Agreement (as defined below) entered into by and between the customer located solely within the United State set forth below (hereinafter referred to as “LEA”) and Code.org (hereinafter referred to as “Provider”) effective as of the date the DPA is accepted by LEA (“Effective Date”) (each of Provider and LEA, a “Party” and together “Parties”). The Parties agree to the terms as stated herein.

### RECITALS

**WHEREAS**, the Provider has agreed or will agree to provide the LEA with certain digital educational services as described in Section 1 pursuant to the Code.org Terms of Service located at <https://code.org/tos> (the “Service Agreement”) entered into the same date as this DPA; and

**WHEREAS**, in order to provide the Services described in Section 1, the Provider may receive or create and the LEA may provide documents or data that are covered by several applicable federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 et. seq.; and

**WHEREAS**, the documents and data transferred from LEAs and created or accessed by the Provider’s Services are also subject to various state student privacy laws; and

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

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

#### 1. PURPOSE AND SCOPE

- 1.1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit “C”) transmitted to Provider from the LEA and its users pursuant to the Service Agreement including compliance with all applicable federal and state privacy statutes, including the FERPA, PPRA, COPPA, and IDEA. This DPA supplements the Service Agreement and together with the Service Agreement, is collectively referred to as the “Agreement.”
- 1.2. **Nature of Services Provided.** Pursuant to and as fully described in the Service Agreement, Provider has agreed to provide the digital educational services as set forth in Exhibit “A” hereto and any other products and services that Provider may provide now or in the future (the “Services”).
- 1.3. **Student Data to Be Provided.** In order to perform the Services, the Parties shall indicate the categories of Student Data to be provided or collected by the Provider in the Schedule of Data, attached hereto as Exhibit “B”.

---

<sup>1</sup> Modeled After The Student Data Privacy Consortium’s Set Of Baseline Model Clauses

- 1.4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, the Service Agreement, privacy policies or any terms of service with respect to the treatment of Student Data.

## 2. DATA OWNERSHIP AND AUTHORIZED ACCESS

- 2.1. **Student Data Property of LEA.** All Student Data or any other Education Records (as defined on Exhibit “C”) transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent). The Provider further acknowledges and agrees that all copies of such Student Data or Education Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Education Records. The Parties agree that as between them, all rights, including all intellectual property rights, in and to Student Data or Education Records covered per this Agreement shall remain the exclusive property of the LEA or the party who provided such data (such as the student or parent).
- 2.2. **Exemptions under FERPA.** LEA may not generally disclose Personally Identifiable Information from an eligible student’s Education Record to a third-party without written consent of the parent and/or eligible student or without meeting one of the exemptions set forth in FERPA (“FERPA Exemption(s)”), including the exemption for Directory Information (“Directory Information Exemption”) or School Official exemption (“School Official Exemption”). For the purposes of FERPA, to the extent Personally Identifiable Information from Education Records are transmitted to Provider from LEA or from students using accounts at the direction of the LEA, the Provider shall be considered a School Official as defined on Exhibit “C”, under the control and direction of the LEAs as it pertains to the use of Education Records. Additionally, certain information, provided to Provider by LEA about a student, such as student name and grade level, may be considered Directory Information as defined on Exhibit “C” under FERPA and thus not an Education Record.
- 2.3. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information contained in the related student’s Education Records and correct erroneous information, consistent with the functionality of Services. Provider shall cooperate and respond within thirty (30) days to the LEA’s request for Personally Identifiable Information contained in the related student’s Education Records held by the Provider to view or correct as necessary. In the event that a parent/legal guardian of a student, an eligible student or other individual contacts the Provider to review any of the Education Records or Student Data accessed pursuant to the Services, the Provider shall refer the parent, eligible student or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information, provided however, that Provider may also allow for direct access requests (but not correction or deletion rights) of Student Data and/or Education Records from a verified parent.
- 2.4. **Separate Accounts and Outside School Logins.** Students and parent users may have personal or non-school accounts (i.e. for use of Code.org at home not related to school) in addition to school accounts (“Outside School Accounts”). Additionally, they may choose to create personal login information to student accounts to continue developing projects or work outside of school (“Personal Login”). Student Data shall not include information a student or parent provides to Provider through such Outside School Account or use of a

school account with a Personal Login independent of the student's or parent's engagement with the Services at the direction of the LEA. Additionally, If Student Generated Content is stored or maintained by the Provider as part of the Services, Provider may, at the request or with the consent of the parent or legal guardian, transfer said Student Generated Content to a separate student account or the Outside School Account or continue to use such content within the former school account with a Personal Login upon termination of the Service Agreement; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service.

- 2.5. **Third Party Request.** Should a third party, excluding a Service Provider, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall redirect the third party to request the data directly from the LEA, unless and to the extent that Provider reasonably believes it must grant such access to the third party because the data disclosure is necessary: (i) pursuant to a court order or legal process, (ii) to comply with statutes or regulations, (iii) to enforce the Agreement, or (iv) if Provider believes in good faith that such disclosure is necessary to protect the rights, property or personal safety of Provider's users, employees or others. Provider shall notify the LEA in advance of a compelled disclosure to a third party, unless legally prohibited.
- 2.6. **Service Providers.** Provider shall enter into written agreements with all Service Providers performing functions pursuant to this Agreement, whereby the Service Providers agree to protect Student Data in manner no less stringent than the terms of this DPA. The list of Provider's current Service Providers can be accessed through the Provider's Privacy Policy (which may be updated from time to time).

### 3. DUTIES OF LEA

- 3.1. **Provide Data In Compliance With Laws.** LEA shall provide Student Data for the purposes of the Agreement in compliance with any applicable state or federal laws and regulations pertaining to data privacy and security, including, without limitation, the FERPA, PPRA, and IDEA. If LEA is providing Directory Information or any Education Record to Provider, LEA represents, warrants and covenants to Provider, as applicable, that LEA has:
- a. complied with the Directory Information Exemption, including, without limitation, informing parents and eligible students what information the LEA deems to be Directory Information and may be disclosed and allowing parents and eligible students a reasonable amount of time to request that schools not disclose Directory Information about them; and/or
  - b. complied with the School Official Exemption, including, without limitation, informing parents in their annual notification of FERPA rights that the Institution defines "school official" to include service providers and defines "legitimate educational interest" to include services such as the type provided by Provider; or
  - c. obtained all necessary parental or eligible student written consent to share the Student Data with Provider, in each case, solely to enable Provider's operation of the Service.

If LEA is relying on the Directory Information exemption, LEA represents, warrants, and covenants to Provider that it shall not provide information to Provider from any student or parent/legal guardian that has opted out of the disclosure of Directory Information. Provider depends on LEA to ensure that LEA is complying with the



FERPA provisions regarding the disclosure of any Student Data that will be shared with Provider.

- 3.2. **Reasonable Security.** LEA shall employ administrative, physical, and technical safeguards consistent with industry standards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted data from unauthorized access, disclosure or acquisition by an unauthorized person.
- 3.3. **Unauthorized Access Notification.** LEA shall notify Provider immediately, but in no less than 72 hours, of any known or suspected unauthorized use or access of the Services, LEA's account, or Student Data. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized use or access.

#### 4. DUTIES OF PROVIDER

- 4.1. **Privacy Compliance.** The Provider shall comply in all material respects with all applicable state and federal laws and regulations pertaining to data privacy and security, applicable to the Provider in providing the Service to LEA. With respect to Student Data that the LEA permits Provider to collect or access pursuant to the Agreement, Provider agrees to support LEA in upholding LEA's responsibilities with FERPA and PPRA.
- 4.2. **Authorized Use.** Student Data shared pursuant to this Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services and for the uses set forth in the Agreement and/or as otherwise legally permissible, including, without limitation, for adaptive learning or customized student learning. The foregoing limitation does not apply to any De-Identified Data (as defined in Exhibit "C").
- 4.3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.
- 4.4. **No Disclosure.** Provider shall not disclose, transfer, share or rent any Student Data obtained under the Agreement in a manner that directly identifies an individual student to any other entity other than LEA, except: (i) as authorized by the Agreement; (ii) as directed by LEA; (iii) to authorized users of the Services, including parents or legal guardians; (iv) as permitted by law; (v) in response to a judicial order as set forth in Section 2.5; (vi) to protect the safety or integrity of users or others, or the security of the Services; or (vii) to Service Providers, in connection with operating or improving the Service. Provider will not Sell (as defined in Exhibit "C") Student Data to any third party.
- 4.5. **De-Identified Data.** De-Identified Data may be used by the Provider for any lawful purpose, including, but not limited to, development, research, and improvement of educational sites, services, or applications, and to demonstrate the market effectiveness of the Services. Provider's use of such De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Provider agrees not to attempt to re-identify De-identified Data and not to transfer De-identified Data to any party unless that party agrees in writing not to attempt re-identification.
- 4.6. **Disposition of Data.** Provider shall, at LEA's request, dispose of or delete all Personally Identifiable Information contained in Student Data within a reasonable time period following a written request. If no written request is received, Provider shall dispose of or delete all Personally Identifiable Information contained in Student Data at the earliest of (a) when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law. Nothing in the DPA authorizes Provider to maintain

Personally Identifiable Information contained in Student Data obtained under the Agreement beyond the time period reasonably needed to complete the disposition, unless a student, parent or legal guardian of a student chooses to establish and maintain a separate Personal Login with Provider to retain Student Generated Content. Disposition shall include (1) the shredding of any hard copies of any Personally Identifiable Information contained in Student Data; (2) erasing any Personally Identifiable Information contained in Student Data; or (3) otherwise modifying the Personally Identifiable Information contained in Student Data to make it unreadable or indecipherable or De-Identified or maintained to use with a Personal Login pursuant to the other terms of the DPA. Provider shall provide written notification to LEA when the Personally Identifiable Information contained in Student Data has been disposed pursuant to the LEA's request for deletion. The duty to dispose of Student Data shall not extend to data that has been De-Identified. The LEA may employ a "Request for Return or Deletion of Student Data" substantially in the form attached hereto as Exhibit "D".

- 4.7. **Transfer of Student Data to LEA.** If a written request is received from LEA to transfer Personally Identifiable Information contained in Student Data to LEA, Provider shall transfer said Personally Identifiable Information contained in Student Data to LEA or LEA's designee within sixty (60) days of the date of such written request by LEA, or as required by law, and according to a schedule and procedure as the Parties may reasonably agree.
- 4.8. **Advertising Prohibition.** Provider is prohibited from using Personally Identifiable Information contained in Student Data to (a) serve Targeted Advertising to students or families/guardians unless with the consent of parent/guardian or LEA; (b) develop a profile of a student for any commercial purpose other than providing the Service or as authorized by the parent/guardian or LEA; or (c) develop commercial products or services, other than as necessary to provide the Service to LEA, as authorized by the parent or legal guardian, or as permitted by applicable law. This section shall not be construed to (i) limit the ability of Provider to use Student Data for adaptive learning or customized student learning purposes (including generating personalized learning recommendations for account holders or sending Program Communications to account holders); (ii) prohibit Provider from using aggregate or De-Identified Data to inform, influence or enable marketing, advertising or other commercial efforts by Provider, (iii) prohibit Provider from marketing or advertising directly to parents or other users so long as the marketing or advertising did not result from the use of Personally Identifiable Information contained in Student Data obtained by Provider from providing the Services; (iv) prohibit Provider from using Student Data to recommend educational products or services to parents/guardians, students or LEA's so long as the recommendations are not based in whole or part by payment or other consideration from a third party; (v) prohibit Provider from using Student Data with parent/guardian consent to direct advertising to students to identify higher education or scholarship providers that are seeking students who meet specific criteria.

## 5. DATA SECURITY AND DATA BREACH

- 5.1. **Data Security.** The Provider agrees to employ administrative, physical, and technical safeguards consistent with industry standards designed to protect Student Data from unauthorized access, disclosure, use or acquisition by an unauthorized person, including when transmitting and storing such information. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "E" hereto. These measures shall include, but are not limited to:

- a. **Passwords and Employee Access.** Provider shall secure usernames, passwords,

and any other means of gaining access to the Services or to Student Data, at a level consistent with Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees, contractors or Service Providers that are performing the Services.

- b. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data, including ensuring that Student Data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student Data obtained or generated pursuant to the Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Agreement except as necessary to provide the Service, to fulfill data requests by LEA or as otherwise set forth in the Agreement. The foregoing does not limit the ability of the Provider to disclose information as permitted under Section 2.5 or to allow any necessary Service Providers to view or access data as set forth in Section 4.4.
- c. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the Services.
- d. **Security Technology.** When the Service is accessed using a supported web browser, Secure Socket Layer (“SSL”), or equivalent technology shall be employed to protect Student Data from unauthorized access. The security measures employed shall include server authentication and data encryption at rest and in transit. Provider shall host Student Data pursuant to the Agreement in an environment using a firewall that is maintained according to industry standards.
- e. **Security Coordinator.** The name and contact information of each Party’s designated representative for the purposes of matters relating to security of Student Data received pursuant to the Agreement is set forth below:
  - i. Provider’s security coordinator (“Security Coordinator”) is: Bryan Djunaedi [insert].
  - ii. LEA’s designated representative of matters relating to security of Student Data is set forth on the signature page of this DPA.
- f. **Service Provider Bound.** Provider shall enter into written agreements whereby Service Providers agree to secure and protect Student Data in a manner no less stringent than the terms of this Section 5. Provider shall periodically conduct or review compliance monitoring and assessments of Service Providers to determine their compliance with this Section 5.

5.2. **Data Breach.** In the event that Provider becomes aware of any actual or reasonably suspected unauthorized disclosure of or access to Student Data (a “Security Incident”), Provider shall provide notification to LEA as required by the applicable state law, but in no event later than thirty (30) days of the incident (each a “Security Incident Notification”) Provider shall follow the following process:

- a. Unless otherwise required by the applicable law, the Security Incident Notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
- b. The Security Incident Notification described above in Section 5.2(a) shall include such information required by the applicable state law, and at a minimum, the following information, to the extent available:



- i. The name and contact information of the reporting Provider subject to this section.
  - ii. A list of the types of Personally Identifiable Information that were or are reasonably believed to have been the subject of the Security Incident.
    - If the information is possible to determine at the time the notice is provided, then either (1) the date of the Security Incident, (2) the estimated date of the Security Incident, or (3) the date range within which the Security Incident occurred. The Security Incident Notification shall also include the date of the notice.
  - iii. Whether, to the knowledge of Provider at the time the Security Incident Notice was provided the notification was delayed as a result of a law enforcement investigation
  - iv. A general description of the Security Incident, if that information is possible to determine at the time the notice is provided.
- c. At Provider's discretion, the Security Incident Notification may also include any of the following:
  - i. Information about what the Provider has done to protect individuals whose Personally Identifiable Information has been breached by the Security Incident.
  - ii. Advice on steps that the person whose Personally Identifiable Information has been breached may take to protect himself or herself.
- d. Provider agrees to adhere to all requirements applicable to Provider providing the Service in applicable State and federal law with respect to a Security Incident related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such Security Incident.
- e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a Security Incident involving Student Data or any portion thereof, including Personally Identifiable Information ("Incident Response Plan") and agrees to provide LEA, upon request, with a copy of the Incident Response Plan or a summary of such Incident Response Plan to the extent such plan includes sensitive or confidential information of Provider.
- f. To the extent LEA determines that the Security Incident triggers third party notice requirements under applicable laws, Provider will cooperate with LEA as to the timing and content of the notices to be sent. Except as otherwise required by law, Provider will not provide notice of the Security Incident directly to individuals whose Personally Identifiable Information was affected, to regulatory agencies, or to other entities, without first providing written notice to LEA. This provision shall not restrict Provider's ability to provide separate security breach notification to customers, including parents and other individuals with Outside School Accounts.

## 6. MISCELLANEOUS

- 6.1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or as required by law.

- 6.2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by terminating the Service Agreement as set forth therein. The LEA or Provider may terminate this DPA and the Service Agreement in the event of a material breach of the terms of this DPA.
- 6.3. **Effect of Termination Survival.** If the Service Agreement is terminated (thereby terminating this DPA), the Provider shall dispose of all of LEA's Personally Identifiable Information contained in Student Data following the procedures set forth in Section 4.6, which includes De-Identification.
- 6.4. **Priority of Agreements.** This DPA shall govern the treatment of Student Data. With respect to the treatment of Student Data, in the event there is conflict between the terms of the DPA, the Service Agreement, or any other agreement between Provider and LEA, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement, or any other agreement shall remain in effect, including, without limitation, any license rights, limitation of liability or indemnification provisions.
- 6.5. **Notice.** All notices or other communication required or permitted to be given under this DPA must be in writing and given by e-mail transmission, sent to the designated representatives listed below:

The designated representative for the Provider for this DPA is:

Privacy Office

email: [privacy@code.org](mailto:privacy@code.org)

The designated representative for the LEA for this DPA is the individual who enters into the DPA and provides his or her relevant email address (online) during the acceptance process.

- 6.6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege. For clarity, nothing in this Section prohibits Provider from amending the Service Agreement pursuant to the amendment provisions set forth therein.
- 6.7. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
- 6.8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE

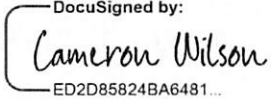


LEA SIGNING THE DPA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY THE LEA RESIDES IN, OF THE STATE OF THE LEA SIGNING THE DPA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

- 6.9. **Waiver.** No delay or omission of the LEA or Provider to exercise any right hereunder shall be construed as a waiver of any such right and the LEA or Provider (as applicable) reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
- 6.10. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.
- 6.11. **Electronic Signature:** The Parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with applicable state and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of their electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.
- 6.12. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

*[Signatory Information Follows]*

**CODE.ORG**

By: DocuSigned by:  
Cameron Wilson  
ED2D85824BA6481...

Name: Cameron Wilson

Title: Chief Operating Officer

Address: 1501 Fourth Avenue, Suite 900  
Seattle, WA 98101

Date: 6/12/2020 | 12:25:01 PDT

**LEA**

By:

Authorized Representative:

Title:

Address:

Date:

SAMPLE

## EXHIBIT "A"

### DESCRIPTION OF SERVICES

Code.org is a nonprofit dedicated to expanding participation in computer science by making it available in more schools, and increasing participation by women and underrepresented students of color.

As part of its mission to expand access to computer science Code.org provides the following services and resources:

- An online curriculum for teaching computer science, and an online learning platform for students to learn coding and computer science and to display and share their work
- Professional learning program for teachers to prepare to teach computer science
- Resources to support schools, districts, teachers, administrators, students, volunteers, parents, and advocates who want to expand the availability of computer science education, including recommendations of third party curriculum and course providers, links to educational resources, etc.
- Information about the state of computer science education in K-12 schools in America and globally
- Advocacy in support of Computer Science education in the K-16 education system
- The coordination and leadership of the global Hour of Code campaign for celebrating participation in computer science

# EXHIBIT "B"

## SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify: standard log files, web beacons, and pixel tags	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify: Student answers to assessments in Code.org coursework	X
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth (year only)	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, preferred or primary language spoken by student)	X
	Other demographic information-Please specify: Age	X
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
Student Contact Information	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Identifiers	Address	
	Email (used temporarily to recover an account, not stored)	X
	Phone	
Student In App Performance	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	X
	Student app username	X
Student Program Membership	Student app passwords	X
	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures, projects etc.	X

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	

Category of Data	Elements	Check if used by your system
(Other)		
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify	

	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

SAMPLE

## EXHIBIT “C”

### DEFINITIONS

**“De-Identified Data”** means information that has all Personally Identifiable Information, including direct and indirect identifiers removed or obscured, such that the remaining information does not reasonably identify an individual. This includes, but is not limited to, name, date of birth, demographic information, location information and school identity.

**“Directory Information”** shall have the meaning set forth under FERPA cited as 20 U.S.C. 1232 g(a)(5)(A)

**“Education Record”** shall have the meaning set forth under FERPA cited as 20 U.S.C. 1232 g(a)(4)

**“Indirect Identifiers”** means any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty.

**“NIST 800-63-3”** shall mean the National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

**“Personally Identifiable Information” or “PII”** means data, including Indirect Identifiers, that can be used to identify or contact a particular individual, or other data which can be reasonably linked to that data or to that individual’s specific computer or device. Student PII includes, without limitation, those items set forth in the definition of PII under FERPA. When anonymous or non-personal information is directly or indirectly linked with Personally Identifiable Information, the linked non-personal information is also treated as personal information. Persistent identifiers that are not anonymized, De-Identified or aggregated are personal information.

**“Program Communications”** shall mean in-app or emailed communications relating to Provider’s educational services, including prompts, messages and content relating to the use of the Service, 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 Service, service updates (for example new features or content, including using for at-home learning opportunities), and information about special or additional programs (e.g. the Hour of Code) offered through the Services or Code.org website or application.

**“Sell”** consistent with the Future of Privacy Forum Student Privacy Pledge, 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 DPA with respect to the previously acquired Personally Identifiable Information contained in Student Data. Sell also does not include sharing, transferring or disclosing Student Data with a Service Provider 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 Service Provider does not Sell the Student Data except as necessary to perform the business purpose. Provider is also not “selling” personal information if (i) a user directs Provider to intentionally disclose Student Data, (ii) if a parent or other user (with parent consent) purchases Student Data (e.g. enhanced reports) or if (iii) a user uses Code.org to intentionally interact with a third party, provided that such third party also does not Sell the Student Data.

**“Service Provider”** means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its Services, and who has access to PII.



**“School Official”** means for the purposes of this DPA and pursuant to FERPA (34 CFR 99.31 (B)), a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Education records; and (3) Is subject to FERPA (34 CFR 99.33(a)) governing the use and re-disclosure of personally identifiable information from Education Records.

**“Student Data”** means any Personally Identifiable Information, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians, for a school purpose, that is descriptive of the student including, but not limited to, information in the student’s Educational Record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifiers, search activity, photos, voice recordings or geolocation information. To the extent U.S. law applies, Student Data may include Education Records. Student Data as specified in Exhibit “B” is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not include De-Identified Data or information that has been anonymized, or anonymous usage data regarding a student’s use of Provider’s Services.

**“Student Generated Content”** means materials or content created by a student including content created at the direction of the LEA personnel or during classroom use of the Services, such as, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content. “Student Generated Content” does not include student responses to a standardized assessment where student possession and control would jeopardize the validity and reliability of that assessment.

**“Targeted Advertising”** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time and across non-affiliate websites for the purpose of targeting subsequent advertising. “Targeted Advertising” does not include advertising to a student based on the content of a web page, search query or a user’s contemporaneous behavior on the web site or a response to a student’s response or request for information or feedback, both of which are permitted.

**EXHIBIT "D"**

**DIRECTIVE FOR DISPOSITION OF STUDENT DATA**

LEA directs Code.org to dispose of Student Data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

*[Insert categories of data here]*

☐ Disposition is Complete. Disposition extends to all categories of Student Data.

2. Nature of Disposition

☐ Disposition shall be by destruction or deletion of Student Data, including De-Identification of Student Data as set forth in Section 4.6 ("Disposition of Data").

☐ Disposition shall be by a transfer of Student Data. The Student Data shall be transferred to the following site as follows:

[Provide directions of where data files should be sent or uploaded]

3. Timing of Disposition

Student Data shall be disposed of by the following date:

☐ As soon as commercially practicable

4. Signature

(Authorized Representative of LEA)

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Company

Date

SAMPLE

**EXHIBIT “E”**  
DATA SECURITY REQUIREMENTS

Please see our Security Whitepaper for details:  
<https://code.org/about/InformationSecurityPolicy.pdf>

SAMPLE



# WOODFORD COUNTY PUBLIC SCHOOLS

330 Pisgah Pike • Versailles, Kentucky 40383-9214 • (859) 879-4600

Danny Adkins, Superintendent

## *Memorandum of Agreement: Data Sharing Agreement*

### **Introduction**

- This document is an agreement between the Woodford County Public Schools (WCPS) and Renaissance Learning, Inc. (hereinafter “the contracting party”) regarding the transfer of student and teacher data to the contracting party and the subsequent processing of that data.
- This agreement excludes any data which is freely and publicly available through other sources.
- Pursuant to KRS 61.932 and KRS 365.734, the parties to this agreement do hereby agree to the following:

### **Mechanism for Data Sharing**

WCPS and the contracting party will at the appropriate time agree on a file or data sharing process that will involve the transfer of the data via the public networks.

### **Obligations of the contracting party**

#### **The contracting party warrants that it will:**

- Use this data only for the joint project outlined above.
- Read and strictly comply with the provisions of the Family Educational Rights and Privacy Act (“FERPA”) and KFERPA; KRS 160.700 *et seq.* While in possession of this data maintain it in a secure, non-public location.
- Ensure that the student data will be accessed, used and manipulated **only** by those individuals necessary for the successful implementation of the project.
- Advise all individuals accessing the data on proper procedures for securely maintaining the data.
- Take appropriate technical and organizational measures against the unauthorized or unlawful accessing of the data.
- Securely delete all copies of the student data upon receipt of written request from WCPS at the end of the Services Agreement, or within a reasonable amount of time, when after they are no longer required to provide the services. “Securely delete” means that industry standard methods will be taken for the purpose of ensuring that no unauthorized person shall be able to reasonably locate or extract the data after the deletion date.
- Promptly-After receipt of comply with any request from WCPS to amend, transfer or delete the data or a subset thereof, the contracting party will evaluate the amount of time needed to complete the request and provide WCPS with an estimate of completion. For some of its products and services, the contracting party may be unable to delete all data from the WCPS account during the middle of the services agreement term. If the contracting party is unable to delete certain data, the contracting party shall promptly notify WCPS with an estimated deletion time and identification of such data.
- The contracting party 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 purpose, and shall not sell, disclose, or otherwise process student data for any commercial purpose.
- Defend, indemnify, and hold harmless WCPS its agencies, officers and employees from any **and**



~~all claims of any nature party of intellectual property rights infringement and any third party claims arising out of the agreement between WCPS and the contracting party,~~ including all reasonable costs, expenses, and attorney's fees, which may in any manner result from or arise out of this agreement, except for claims resulting from or arising out of the WCPS' contributory or sole negligence. The legal defense provided by the contracting party to WCPS under this provision must be free of any conflicts of interest, even if retention of separate legal counsel for the WCPS is necessary. The contracting party also agrees to defend, indemnify, and hold WCPS harmless for all reasonable costs, expenses, and attorneys' fees finally awarded by a court or that are included in a settlement entered into by the parties. WCPS agrees to notify the contracting party of such a claim within ~~a reasonable time~~ seven business days and agrees to cooperate with the contracting party in the defense and any related settlement.

#### **Data Breach Act**

Pursuant to KRS 61.931, *et seq.*, the contracting party warrants it has procedures and practices in place to safeguard against security breaches.

In the event of a confirmed security breach, the contracting party shall notify the WCPS promptly and no more than within 48 hours ten (10) business days ~~of after~~ the ~~suspected or~~ confirmed breach, and the contracting party shall begin conducting a reasonable and prompt investigation to determine whether the security breach has resulted in or is likely to result in the misuse of personal information.

Within ~~48 hours~~ ten (10) business days of completion of the investigation, the contracting party shall notify the above if the investigation finds that the misuse of personal information occurred or is likely to occur.

#### **Data Opt Out**

WCPS may provide a mechanism for students, parents or guardians to opt out of any data sharing agreement with any contracting party.

\_\_\_\_\_  
WCPS Superintendent

\_\_\_\_\_  
Contracting Party Representative

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date





Tincher, Holly <holly.tincher@woodford.kyschools.us>

---

## Re: Welcome to Renaissance - 95471 - Huntertown Elementary School

---

Vessels, Emily <Emily.Vessels@dinsmore.com>  
To: "Tincher, Holly" <holly.tincher@woodford.kyschools.us>

Thu, Dec 5, 2024 at 1:14 PM

Those changes are acceptable. Thank you !



### Emily H. Vessels

Associate

Dinsmore & Shohl LLP • Legal Counsel

101 South Fifth Street

Suite 2500

Louisville, KY 40202

T (502) 540-2374 • F (502) 585-2207

E [Emily.Vessels@DINSMORE.COM](mailto:Emily.Vessels@DINSMORE.COM) • [dinsmore.com](http://dinsmore.com)

**From:** Tincher, Holly <holly.tincher@woodford.kyschools.us>

**Sent:** Thursday, December 5, 2024 11:06 AM

**To:** Vessels, Emily <Emily.Vessels@DINSMORE.COM>

**Subject:** Fwd: Welcome to Renaissance - 95471 - Huntertown Elementary School

Hi Emily -

Please look over the attached file - Renaissance has another small revision to the data sharing agreement for you to review.

Thanks,

**Holly Tincher**

Systems Analyst

Woodford County Schools

859-879-4600 ext 2131

| |

----- Forwarded message -----

From: **Connor Gray** <connor.gray@renaissance.com>

Date: Thu, Dec 5, 2024 at 11:03 AM

Subject: Re: Welcome to Renaissance - 95471 - Huntertown Elementary School

To: Tincher, Holly <holly.tincher@woodford.kyschools.us>



Hey! One more revision from our team highlighted in yellow. Please review.

If acceptable, our team will provide a signed copy. Please let me know if you have any questions!

**Connor Gray (he/him/his)**

Account Manager | Mississippi

M: (601) 914-2583

[Click here to schedule a meeting](#)

[www.renaissance.com](http://www.renaissance.com) | [Renaissance Privacy Policy](#) | [Unsubscribe](#)

---

**From:** Tincher, Holly <[holly.tincher@woodford.kyschools.us](mailto:holly.tincher@woodford.kyschools.us)>

**Sent:** Tuesday, December 3, 2024 6:49 AM

**To:** Connor Gray <[connor.gray@renaissance.com](mailto:connor.gray@renaissance.com)>

**Subject:** Re: Welcome to Renaissance - 95471 - Huntertown Elementary School

**Caution:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi Connor -

I received the DSA back from our Board attorney. She has made a few edits in the attached copy.

**Holly Tincher**

Systems Analyst

Woodford County Schools

(859) 879-4600 ext 2131

On Mon, Dec 2, 2024 at 9:00 AM Connor Gray <connor.gray@renaissance.com> wrote:

Good Morning Holly,

Our contracts team returned the Data Sharing Agreement with the following message.

Please let me know if you have any questions!

"We do need to request some edits in the DPA proposed by the Customer. Attached is the redlined DPA for you to share back with the Customer. If they can agree to our changes, I can prepare a signed version of the document for you to send back as well. Let me know of any questions. Thanks."

Error!  
Filename  
not  
specified.

**Connor Gray (he/him/his)**

Account Manager | Mississippi

M: (601) 914-2583

Error! Filename not specified. Error! Filename not specified. Error! Filename not specified. Error! Filename not specified.

[Click here to schedule a meeting](#)

Error! Filename not specified.

[www.renaissance.com](http://www.renaissance.com) | [Renaissance Privacy Policy](#) | [Unsubscribe](#)

---

**From:** Tincher, Holly <holly.tincher@woodford.kyschools.us>

**Sent:** Friday, November 22, 2024 6:50 AM

**To:** Connor Gray <connor.gray@renaissance.com>

**Subject:** Re: Welcome to Renaissance - 95471 - Huntertown Elementary School

**Caution:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi Connor -

I apologize! I missed this email on Monday. Attached is a copy of our district's standard data sharing agreement.

Holly Tincher

Systems Analyst

Woodford County Schools

859-879-4600 ext 2131

On Mon, Nov 18, 2024 at 4:41 PM Connor Gray <connor.gray@renaissance.com> wrote:

Good Afternoon Holly,

Yes! I can certainly assist in completing your Data Sharing Agreement. Please send it my way!

Yes, once you are ready, please assign Freckle ELA, Math, Science, and Social Studies to Darren.

Originally, this was intended to be a classroom license. Our classroom licenses are only able to be purchased via credit card. In order to fulfill the order via purchase order, I had to build a custom quote. Our campus minimum is for 100 licenses; thus, there will likely be additional licenses that can be shared within the school. Feel free to assign the extra licenses as requested.

Best,



Connor Gray (he/him/his)

Account Manager | Mississippi

M: (601) 914-2583



[Click here to schedule a meeting](#)

Renaissance

See Every Student.

[www.renaissance.com](http://www.renaissance.com) | [Renaissance Privacy Policy](#) | [Unsubscribe](#)

[Quoted text hidden]

**Disclaimer:** The information contained in this communication may be confidential, is intended only for the use of the recipient(s) named above, and may be legally privileged. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication, or any of its contents or attachments, is strictly prohibited. If you have received this communication in error, please return it to the sender immediately and delete the original message and any copy of it from your computer system. If you have any questions concerning this message, please contact the sender. Emails sent to and from Renaissance Learning, Inc. and its affiliates are monitored and subject to disclosure, including in connection with regulatory or other legal proceedings.

**Disclaimer:** The information contained in this communication may be confidential, is intended only for the use of the recipient(s) named above, and may be legally privileged. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication, or any of its contents or attachments, is strictly prohibited. If you have received this communication in error, please return it to the sender immediately and delete the original message and any copy of it from your computer system. If you have any questions concerning this message, please contact the sender. Emails sent to and from Renaissance Learning, Inc. and its affiliates are monitored and subject to disclosure, including in connection with regulatory or other legal proceedings.

**Disclaimer:** The information contained in this communication may be confidential, is intended only for the use of the recipient(s) named above, and may be legally privileged. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication, or any of its contents or attachments, is strictly prohibited. If you have received this communication in error, please return it to the sender immediately and delete the original message and any copy of it from your computer system. If you have any questions concerning this message, please contact the sender. Emails sent to and from Renaissance Learning, Inc. and its affiliates are monitored and subject to disclosure, including in connection with regulatory or other legal proceedings.

---

**NOTICE:** This electronic mail transmission from the law firm of Dinsmore & Shohl may constitute an attorney-client communication that is privileged at law. It is not intended for transmission to, or receipt by, any unauthorized persons. If you have received this electronic mail transmission in error, please delete it from your system without copying it, and notify the sender by reply e-mail, so that our address record can be corrected.

**WOODFORD COUNTY BOARD OF EDUCATION  
AGENDA ITEM**

**ITEM #:**           **DATE:** December 5, 2024

**TOPIC/TITLE:** Fire Science Pathway MOU between WCPS and City of Versailles

**PRESENTER:** Ryan Asher 

**ORIGIN:**

- ☐ TOPIC PRESENTED FOR INFORMATION ONLY (No board action required.)
- ☒ ACTION REQUESTED AT THIS MEETING
- ☐ ITEM IS ON THE CONSENT AGENDA FOR APPROVAL
- ☐ ACTION REQUESTED AT FUTURE MEETING:            (DATE)
- ☒ BOARD REVIEW REQUIRED BY

- ☐ STATE OR FEDERAL LAW OR REGULATION
- ☒ BOARD OF EDUCATION POLICY
- ☐ OTHER:

**PREVIOUS REVIEW, DISCUSSION OR ACTION:**

- ☐ NO PREVIOUS BOARD REVIEW, DISCUSSION OR ACTION
- ☒ PREVIOUS REVIEW OR ACTION

- ☒ DATE: 9/23/24
- ☒ ACTION: Report given as part of Instructional Update by R. Asher

**BACKGROUND INFORMATION:**

WCPS has been working in collaboration with Chief Rankin of the Versailles Fire Department to establish a Fire Science Pathway for WCHS students. This opens up a new opportunity for our students as these pathway courses are not currently offered locally. This also serves as a workforce development for the firefighting field in Versailles and Woodford County.

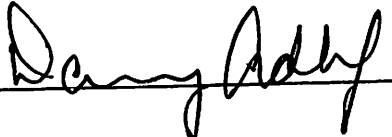
**SUMMARY OF MAJOR ELEMENTS:**

The purpose of this Memorandum of Understanding (MOU) is to define the relationship between the Woodford County Public School (WCPS) and the City of Versailles (COV) in providing instructors for the Fire Science Career Pathway for the 2025-2026 school year. The COV agrees to provide trained and approved professionals to WCPS under the terms and conditions set forth in this MOU.

**IMPACT ON RESOURCES:** Specified in the MOU. The salary reimbursement of \$40,000 will be paid from CTE supplemental funds for 2025-2026.

**TIMETABLE FOR FURTHER REVIEW OR ACTION:**

**SUPERINTENDENT'S RECOMMENDATION:** ☒ Recommended            ☐ Not Recommended

  
\_\_\_\_\_

Memorandum of Understanding  
Fire Science Career Pathway

This Memorandum of Understanding is entered into this 16th day of December, 2024, by and between:

Woodford County Public Schools  
330 Pisgah Pike  
Versailles, KY 40383

And

City of Versailles  
196 South Main Street  
Versailles, KY 40383

The purpose of this Memorandum of Understanding (MOU) is to define the relationship between the Woodford County Public School (WCPS) and the City of Versailles (COV) in providing instructors for the Fire Science Career Pathway for the 2025-2026 school year. The COV agrees to provide trained and approved professionals to WCPS under the terms and conditions set forth in this MOU.

The parties hereby agree to the following terms and conditions:

Woodford County Public Schools (WCPS)

WCPS agrees to:

1. Provide the classroom and shop/bay area for the COV to perform education to the WCPS students and provide a contact person to the COV who will be responsible for the classroom.
2. Provide the necessary books/eBooks for the COV to teach fire science career education to the WCPS students.
3. Provide consumables, if necessary, for the COV to teach fire science career education to the WCPS students. Consumables include, but are not limited to, necessary training supplies for the fire science career education class. Any operating budget for this Agreement is subject to Board approval.

The City of Versailles (COV)

The COV agrees to:

1. Provide a qualified and competent instructor for the fire science career education class.
2. Loan equipment as necessary for the class.

### Financing of the Fire Science Instructor Position

For the 2025-2026 school year, the financing of the instructor position will be as follows:

1. WCPS will reimburse the COV for the instructor's salary in the amount of \$40,000. The COV shall invoice WCPS yearly for the WCPS portion of the instructor's salary. Each invoice is subject to Board approval.
2. COV will be responsible for providing the instructor's salary and employee benefits.
3. Funding responsibilities for subsequent years will be negotiated between WCPS and the COV. Each entity shall be responsible for adjusting their portion of the salary or reimbursement if any adjustments are made for WCPS teachers or COV Fire Employees.

### Employment status of the Fire Science Instructor

The Fire Science Instructor shall remain an employee of the COV Fire Department, and shall not be an employee of WCPS. WCPS and the COV acknowledge that the Instructor shall remain responsive to the chain of command of the COV Fire Department.

WCPS shall not be liable for damage to the instructor's vehicle using parking facilities associated with WCPS, including theft, collision, fire, or any other damage to such vehicle and WCPS shall not be responsible for items left in such vehicle.

WCPS requires the instructor to maintain adequate insurance during the Agreement, including for any loss or damage incurred by the instructor arising from illness or injury suffered in the course of the travel specified in this Agreement.

To the extent allowed by Kentucky state law, WCPS shall be responsible for all liability, injury to persons or property, damages, claims, and expenses arising from use of WCPS facilities by the COV, which are attributable to the actions, negligence or misconduct of WCPS. COV shall be responsible for all liability injury to persons or property, damages, claims and expenses arising from use of WCPS facilities by COV, which are attributable to the actions, negligence or misconduct of COV.

### Insurance

WCPS agrees to provide the COV with a copy of a certificate of insurance indicating that WCPS has a Comprehensive General Liability Insurance Policy providing insurance for use of the WCPS facilities by COV and its officers, employees, agents and invitees, with limits of no less than the following amounts:

Bodily Injury: \$1,000,000 per occurrence  
\$2,000,000 aggregate

Property Damage: \$1,000,000 per occurrence  
\$2,000,000 aggregate

### Time of Performance

This MOU shall be effective from the date of signing and continue in effect indefinitely. Either party may terminate this MOU at any time by giving a 30 day written notice on intention to the other party. If WCPS requests termination during an annual term, WCPS shall pay the prorated share of the instructor's salary for instruction provided up to the date of termination, in accordance with the payment amount set forth in this MOU. This MOU may be immediately terminated upon written consent of all parties.

---

Woodford County Public Schools

---

City of Versailles





Date: 12/6/2024

## Business Agreement

If Agreement is not executed, pricing will expire on: 1/5/2025

Paperwork Prepared By: Chris DeVine

Customer Name	WOODFORD COUNTY SCHOOL DISTRICT - NEW HIGH SCHOOL LOCATION	Subscriber ID	2324414
Physical Address	145 SCHOOL HOUSE RD VERSAILLES, KY 40383	Billing Address	WOODFORD COUNTY SCHOOL DISTRICT 330 PISGAH PIKE VERSAILLES, KY 40383
Primary Contact: Josh Rayburn		Contact to Receive Metronet Text Alerts:	
Primary Contact Number: 859-879-4617		Contact Phone Number:	
Primary Contact Email: josh.rayburn@woodford.kyschools.us		Contact Email Address:	
Referring Customer:		Referring Customer Subscriber ID:	
Referring Partner:			

Service Agreement Term: 36 month(s)

### Voice

QTY	PRODUCT NAME	DESCRIPTION	UNIT PRICE	Monthly Total	One Time Total
1	Business Voice Bundle	Business Voice Service for all customers who require a phone line for office products including fax, POS, and security. Voice Plus/Premium services include mobile applications and enhanced voicemail with transcription.	\$0.00	\$0.00	\$0.00
1	Business Voice Basic	Analog line best suited for office systems including security systems, alarms, elevators, credit card readers, and fax machines.	\$25.65	\$25.65	\$0.00

Monthly Net Total: \$25.65

### Terms & Conditions

By signing this Business Agreement, Customer ("you") acknowledges that Customer has had an opportunity to read and review the terms and conditions of this Business Agreement, and all Metronet terms and conditions applicable to the services that are referenced herein, including our Business Terms and Conditions, our tariff, our Acceptable Use and Privacy Policy ("AUPP"), our Additional Terms of Service Addendum ("Business"), our Managed Wi-Fi Terms of Service, any Statement of Work ("SOW"), Letters of Authorization, and any other terms and conditions that govern the services specifically included in this Business Agreement (all such documents relating to Customer's Services are collectively the "Agreement"). Customer agrees to abide by the Agreement's terms and conditions as amended or updated from time to time. The Agreement can be found at [www.metronet.com/terms-conditions](http://www.metronet.com/terms-conditions) and constitutes the entire agreement between Customer and Metronet with respect to the Services.

Signature:	<i>Banny Adkins</i>
Title:	E66D993250FFD7D4A0989F89D5EED505 readySign Superintendent
Date:	12/06/2024



## STATEMENT OF WORK

Customer Name	WOODFORD COUNTY SCHOOL DISTRICT - NEW HIGH SCHOOL LOCATION
Subscriber ID	
Physical Address	145 SCHOOL HOUSE RD, VERSAILLES, KY 40383

### Explanation Of Work To Be Done

**Note:** If you are submitting an order for Symmetrical Internet Circuits, HPBX, WAN, Wi-Fi etc., it's critical to follow the process for **Complex Orders** and first engage Sales Engineering.

Metronet to install a new Basic Business Analog line for use with the elevator line at the New Woodford County High School at: 145 School House Road, Versailles, KY 40383. Metronet to assign a new number for use with the Elevator. Main on site technical contact for install is: Clay Ratliff: 859-585-1139.

### Day of Service Installation

Metronet will assign an installation date for your Fiber Services. On the Installation Date you will experience service down time due to factors outside of our control. In some cases, this may mean you may not have phone or computer service for several hours. Such downtime is unavoidable, but we will use commercially reasonable efforts to minimize the inconvenience to you.

### DMARC (ONT)

When an ONT/fiber drop is installed MetroNet is responsible for service up to the DMARC (ONT). Anything beyond the DMARC is the customer's internal network and the **business owner's financial responsibility** to contact an IT vendor for support and/or repairs.

### Customer Phone Vendor / Cut Sheet

Phone Vendor Name:	Self
--------------------	------

Customer designates the above mentioned Phone Vendor to be responsible for maintaining the internal phone systems on behalf of Customer. Phone Vendor will be responsible for locating all lines prior to the Installation Date provided by MetroNet and will be responsible for connecting Customer's internal phone system to MetroNet's demarcation point. Phone Vendor must be present on the Installation Date at the designated time. **Customer will be responsible for scheduling the Phone Vendor on the Installation Date and shall pay all expenses associated with the Phone Vendor.** MetroNet will provide Customer with a document detailing the lines/circuits to be installed for the benefit of the Phone Vendor ("Cut Sheet")

### Compliance with Law and Regulations; Usage Policies and Prohibitions

By using any Service, you agree to comply with all applicable laws and regulations, including but not limited to any law or regulation related to call recording or monitoring. Our unlimited long distance plan and other plans where you receive a number of long distance minutes without charge are limited to calls within the 50 United States, Canada and US Territories. Toll-free, trunking, dialing outside of the 50 United States, Canada and US Territories, and call center usages are not included in unlimited or free minutes. In addition to any restrictions of use set forth in our AUPP, you may not use the phone service for any of the following: (i) autodialing, mass communications, spamming, or continuous or excessive calling/texting or call forwarding; (ii) fax broadcast or fax blasting; (iii) telemarketing or solicitations including, without limitation, polling, political solicitation, or charitable solicitation; (iv) unlawful activities, including, but not limited to, unlawful robocalls and/or robotexts; (v) abusive conduct including, without limitation, threatening, harassing or fraudulent behavior; (vi) any purpose that threatens the safety, security or use of our network or our business including, but not limited to, excessive usage, or (vii) uses without live dialog, such as transcription services, intercom or monitoring services. You may not resell our phone service or equipment. If, in our sole discretion, you are placing an abnormally high number of calls, repeatedly placing calls of unusually long duration, placing calls that are harmful or disruptive to our network or our supplier's network or service levels, or using in a prohibited manner any of our phone service features or packages, we reserve the right at our discretion, without advance notice, to charge you for your prior usage conducted in a prohibited manner and/or immediately to suspend, terminate, restrict or non renew your phone service or require you to subscribe to a different phone service package (such as a metered package) as a requirement of continuing your phone service with us. You agree any applicable long distance rates will be calculated based upon the telephone numbers of the calling and called parties and not necessarily the current physical locations of the calling and called parties.

### Changes

Customer understand that any changes made to the SOW or Fiber Services, including but not limited to database information, after execution of this SOW may result in the assignment of a new Installation Date by MetroNet or otherwise delay the provisioning of the Fiber Services to you.

**This SOW is hereby incorporated by reference into the Agreement between Customer and MetroNet, as that term is defined in the terms and conditions. Any capitalized terms not defined herein shall have the same meanings as ascribed to them in the Agreement.**

Name: **Danny Adkins**

Signature: *Danny Adkins*



Date	12/6/2024
Sales Associate	Chris DeVine
Customer	WOODFORD COUNTY SCHOOL DISTRICT - NEW HIGH SCHOOL LOCATION
Subscriber ID	
Address	145 SCHOOL HOUSE RD, VERSAILLES KY 40383

The Primary Contact and Additional Authorized Contacts listed below, have authorization to act on this account (e.g. make billing changes, request changes and upgrades in service/equipment, cancel service, make address changes, request and provide account information, give and accept notices, etc.) whether such action is taken by telephone, electronically or other manner. In the event the Primary Contact or an Additional Authorized Contact ceases to be authorized or a new individual becomes authorized, it is the responsibility of the Primary Contact (or an Additional Authorized Contact in the event of a change in Primary Contact) to provide MetroNet written notice of such change. MetroNet may, but shall have no obligation to, verify authorizations or the identity of the authorizer.

**Primary Contact** will be responsible for **setting up the myMetroNetPortal Account**. Anyone logging in to the business's customer portal account will be able to manage the contacts on your account.

**Primary Contact** will **receive** (and hereby expressly authorizes MetroNet to send) **transactional and/or relationship messages and notifications regarding install Notifications, Payment Notifications, Maintenance Notification, and Service Disruptions via email, text, and phone**. Primary Contact **will have ability to modify this authorization or add/remove additional contacts** in the myMetroNetPortal or by emailing **business-customer-service@metronetinc.com** or calling (855) 769-0936.

**Primary Contact** will be **responsible for managing contacts** in the myMetroNetPortal to receive Install Notifications, Payment Notifications, Maintenance Notification, and Service Disruptions.

## 911 Multi-Line Telephone Systems Notifications

Per FCC regulations, users of Multi-Line Telephone Systems (MLTS) must designate a contact name, phone number and/or email address that will be notified if a 911 call is placed from one of the users' MLTS phones. MetroNet's HPBX phone service is a type of MLTS; therefore, HPBX users must provide and maintain, per FCC regulations, this required information. **If the table below is not completed, the Primary Contact's information will be used by default for all 911 MLTS Notifications.** After your HPBX service is installed, your organization is responsible for managing any changes to your 911 Notification Contact by contacting MetroNet Business Customer Service by email at **business-customer-service@metronetinc.com** or phone at **(855) 769-0936**.

The Contact(s) listed below should be notified if or when a 911 call has been placed from one of my MetroNet HPBX phones. **It is the responsibility of the Primary Contact (or an Additional Authorized Contact in the event of a change in Primary Contact) to keep this Contact List updated.**

## 911 Dispatchable Location Requirements

The FCC has adopted rules to ensure that "Dispatchable Location" is conveyed with 911 calls to dispatch centers placed over Multi-Line Telephone Systems (MLTS). Dispatchable Location means a location that consists of the validated street address of the calling party, plus additional information such as suite, apartment, or similar information necessary to adequately identify the location of the calling party. MetroNet's HPBX phone service is a type of MLTS; therefore, HPBX users must provide and maintain, per FCC regulations, this required information. Before services are installed, you are responsible for providing MetroNet with the Dispatchable Location information associated with your telephone numbers. **After services are installed, you are responsible for updating any changes to your Dispatchable Location information** by contacting Business Customer Service by email **business-customer-service@metronetinc.com** or phone **855-769-0936**.

Primary Contact	Title	Phone	Email
Josh Rayburn	CIO	859-879-4617	josh.rayburn@woodford.kyschools.us
Onsite Contact	Title	Phone	Email
Accounts Payable	Title	Phone	Email
Additional Authorized Contacts	Title	Phone	Email

The undersigned represents and warrants to MetroNet that he/she is authorized to sign this Authorization form on behalf of the Customer.

Name: **Danny Adkins**

Signature: *Danny Adkins*

Company Name	WOODFORD COUNTY SCHOOL DISTRICT - NEW HIGH SCHOOL LOCATION
Address	145 SCHOOL HOUSE RD, VERSAILLES 40383
Contact Name	Josh Rayburn
Contact Phone	859-879-4617

How should out-going Caller ID appear? (15 characters only)

Choose Format - Check all that apply

Listing Options	
None	

## Main Listing Appearance:

Below type EXACTLY how listings will appear in the Directory, including indentions. This information pertains only to the number listed below.

Telephone Number:

Business Pages:

I, \_\_\_\_\_ (Company Representative) attest that the above is accurate and correct. I therefore authorize MetroNet to submit the information as my Directory Listing information.

Name: Danny Adkins	Title: Superintendent
Signature: <i>Danny Adkins</i>	Date: 12/06/2024

E66D993250FFD7D4A0989F89D5EED505

readysign

<b>Date:</b> 12/6/2024
<b>Customer:</b> WOODFORD COUNTY SCHOOL DISTRICT - NEW HIGH SCHOOL LOCATION
<b>Subscriber ID:</b> 2324414

Telephone Number	Description	Hunt on Busy?	Hunt on No Answer?	Hunt Line Position	Hunt Group Voicemail	Basic Voicemail
------------------	-------------	---------------	--------------------	--------------------	----------------------	-----------------

*\*\*Multiple line in Hunt requires Hunt Group Voicemail*

**Special Instructions:**

**MetroNet's Business Complete Phone Includes:**

Long Distance

Caller ID Deluxe

\*66 Repeat Dialing

\*67 Per Call Block

\*69 Call Return

\*72 Call Forwarding

\*75 Speed Calling

\*77 Anonymous Call Rejection

Three Way Calling & Call Waiting (Cannot be combined with Hunting)

***Dedicated Fax Lines will have no features added unless requested***

For additional information regarding MetroNet's Business Complete Phone Features please visit <https://www.metronetinc.com/business/fiber-voice>.

**WOODFORD COUNTY BOARD OF EDUCATION  
AGENDA ITEM**

**ITEM #:**           **DATE:** December 5, 2024

**TOPIC/TITLE:** Safe Harbor Picture Commissions Fundraisers and Strawbridge Student Picture Agreement

**PRESENTER:** Logan Culbertson

**ORIGIN:**

- ☐ TOPIC PRESENTED FOR INFORMATION ONLY (No board action required.)
- ☐ ACTION REQUESTED AT THIS MEETING
- ☒ ITEM IS ON THE CONSENT AGENDA FOR APPROVAL
- ☐ ACTION REQUESTED AT FUTURE MEETING:            (DATE)
- ☐ BOARD REVIEW REQUIRED BY

- ☐ STATE OR FEDERAL LAW OR REGULATION
- ☐ BOARD OF EDUCATION POLICY
- ☐ OTHER:

**PREVIOUS REVIEW, DISCUSSION OR ACTION:**

- ☐ NO PREVIOUS BOARD REVIEW, DISCUSSION OR ACTION
- ☐ PREVIOUS REVIEW OR ACTION

- ☐ DATE:
- ☐ ACTION:

**BACKGROUND INFORMATION:**

Safe Harbor has utilized Strawbridge Studios for student pictures in the Fall and Spring each year.


**SUMMARY OF MAJOR ELEMENTS:**

A commission of sales for student orders was received. We would like to place in the district activity fund to purchase items for student rewards or school store. We would like permission to approve Strawbridge for student picture usage for the next 3 years.

**IMPACT ON RESOURCES:** \$300-\$500 over the next 3 years.

**TIMETABLE FOR FURTHER REVIEW OR ACTION:**

**SUPERINTENDENT'S RECOMMENDATION:** ☒ Recommended            ☐ Not Recommended







# Portrait Renewal Agreement

☐ 1 Year ☐ 2 Years ☐ 3 Years ☐ Bid

## Office Use Only

School #: 111621

School Year: 2026

School: Safe Harbor Academy County: Woodford District: Woodford County School District Phone: (859)879-4694  
Ship Address: 134 Macey Ave. City: Versailles ST: KY Zip: 40383  
Mail Address: 134 Macey Ave. City: Versailles ST: KY Zip: 40383

Title	Name	Email	
Principal	Mr. Logan Culbertson	logan.culbertson@woodford.kyschools.us	Grades at Campus: <u>6-12</u>
			# of Classrooms: <u></u>
			Underclass Enrollment: <u>29</u>
			Senior Enrollment: <u>0</u>
			Mascot: <u>N/A</u>
			Last Day of School: <u></u>

**Strawbridge Studios, Inc. Agrees:** 1. To provide complimentary faculty portraits. 2. To supply each Principal and Secretary with a large desk calendar for the current school year. 3. To guarantee complete satisfaction. The studio agrees to refund complete payment to any student who requests same upon return of their portraits.

Fall Date 08-13-2025 Time  Location  Program 1693 PF-Fall Woodford KY

Notes

Date  Time  Location  Program

Notes

Date  Time  Location  Program

Notes

Date  Time  Location  Program

Notes

Date  Time  Location  Program

Notes

Date  Time  Location  Program

Notes

Date  Time  Location  Program

Notes

Date  Time  Location  Program

Notes

Date  Time  Location  Program

Notes

Date  Time  Location  Program

Notes

Total Sale is based on the total retail price of all commissionable items minus applicable taxes/fees. Due to the cost of production, the agreed upon commission percentage offered may be adjusted if the percentage of sale is lower than the commission percentage offered.

COPYRIGHT - A. The portrait images provided to you are copyright protected and are solely for the use of publishing pictures subject to the terms and conditions of the Terms of Use outlined between the school photography company and the school ("Terms of Use"). Unless otherwise stated in the Terms of Use documentation or with the school photographer's prior written consent, reproduction is limited to use in student management software and yearbooks. You do not have permission to make copies for sale or other distribution in any manner. Terms of Use documentation can be found at [www.strawbridge.net](http://www.strawbridge.net).

**REBOOK BY DEC 15th AND RECEIVE \$100 IN CUSTOM PRINTING**

We will provide you with a \$100 coupon code in June to be used on the Strawbridge Shopify site. Please allow 3-6 weeks for all custom printing requests.

School Representative Signature

Date

Strawbridge Studios Representative

Date

Print Name

Print Name