

RULE 6A-1.0955 AMENDMENT

Lake County School Board

THIS RULE 6A-1.0955 AMENDMENT is made by and between The School Board of Lake County, Florida, a political subdivision of the State of Florida ("**School Board**") and Common Sense Media, a Florida Educational Vendor ("**Provider**"), and intended to modify any agreement previously entered into by School Board and Provider (the "**Prior Agreement**"). School Board and Provider may also be referred to herein each as a "**Party**" and collectively as the "**Parties**".

WHEREAS, School Board is responsible for operating and controlling all public K-12 schools located in Lake County, Florida (collectively referred to herein as "**Lake County Schools**") and is the statutory contracting agent for Lake County Schools.

WHEREAS, Rule 6A-1.0955 of the Florida Administrative Code was promulgated by the Florida Department of Education with an effective date of November 22, 2022 (the "**Rule**").

WHEREAS, the Rule requires certain additional terms and conditions be incorporated into all existing and future agreements that involve or may involve any disclosure or use of student personally identifiable information ("**PII**").

WHEREAS, School Board and Provider believe the Prior Agreement may be subject to the Rule.

NOW, THEREFORE, in consideration of the premises and of the mutual covenants contained herein and to bring the Prior Agreement into compliance with the Rule, the Parties hereby agree to amend and modify the Prior Agreement as follows:

1. The above Recitals are true and correct and are incorporated herein by reference.
2. Attachment "A", including all exhibits attached thereto, is fully incorporated into and made a part of the Prior Agreement.
3. Provider shall promptly notify School Board in writing concerning needed updates to Attachment "A", Exhibit "B" due to any changes that impact the disclosure or use of PII ("**Needed Changes**"), after which the Parties shall modify said Exhibit "B" accordingly. Failure by Provider to notify School Board of any Needed Changes shall constitute default and a material breach of the Prior Agreement and provide School Board the option, but not the obligation, to immediately terminate the Prior Agreement without penalty.
4. The effective date of this Amendment shall be the date of full execution by the Parties.
5. This Amendment may be executed in counterparts, whether signed physically or electronically, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

ATTACHMENT A
STUDENT DATA PRIVACY AGREEMENT

THIS STUDENT DATA PRIVACY AGREEMENT (“SDPA”), as developed by the Student Data Privacy Consortium (“SDPC”) and modified by the local education agency identified herein, is entered into on the date of full execution (the “Effective Date”) by and between The School Board of Lake County, Florida, a political subdivision of the State of Florida and designated local education agency for purpose of this SDPA (“LEA”) and Common Sense Media, a California Educational Vendor. (“Provider”). LEA and Provider may also be referred to herein each as a “Party” and collectively as the “Parties”.

WHEREAS, Provider is obligated under that certain Agreement for Online Educational Services by and between Provider and LEA (the “Service Agreement”), to provide certain educational or digital services to LEA.

WHEREAS, 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).

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

NOW THEREFORE, in consideration of the mutual promises, covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which is acknowledged by the Parties, LEA and Provider hereby agree as follows:

1. The SDPC Standard Clauses, as attached hereto (the “Standard Clauses”), are fully incorporated into and made a part of this SDPA.
2. The following, only if checked, shall be fully incorporated into and made a part of this SDPA (collectively referred to herein as the “Special Provisions”):
 - Supplemental State Terms as set forth in **Exhibit “G”** attached to the Standard Clauses.
 - Additional terms or modifications set forth in **Exhibit “H”** attached to the Standard Clauses.
 - General Offer of Privacy Terms as set forth in **Exhibit “E”** attached to the Standard Clauses.
3. In the event of a conflict between the Standard Clauses and the Special Provisions, the terms of the Special Provisions will control. In the event there is conflict between the terms of the

SDPA and any other writing, including, but not limited to the Service Agreement and any terms of service or privacy policy of Provider, the terms of this SDPA shall control.

4. A description of the services to be provided and the categories of student data that may be provided by LEA to Provider, and other information specific to this SDPA are contained in the Standard Clauses.
5. A description of the services to be provided by Provider to LEA pursuant to this SDPA are contained in **Exhibit "A"** to the Standard Clauses (the "**SDPA Services**").
6. The term of this SDPA shall end on the Expiration Date, as defined in the Service Agreement.
7. 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:

LEA-designated Representative:

Name: Diane Kornegay

Signature: 

Date: 10/19/2023

Title: Superintendent

Address: 201 West Burleigh Blvd, Tavares, FL 32778

Phone: 352-253-6500

Email: KornegayD@lake.k12.fl.us

Provider-designated Representative:

Signature: 

Date: 06 / 15 / 2023

Name: David Kuizenga

Title: Chief Financial & Administrative Officer

Address: 699 8th Street Suite C150, San Francisco, CA 94103

Phone: 917.375.1625

Email: dkuizenga@commonsense.org

SDPC STANDARD CLAUSES

Version 1.0

Article I. ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of SDPA.** The purpose of this SDPA 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 the SDPA Services, Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by LEA. Provider shall be under the direct control and supervision of LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the SDPA Services, LEA shall provide to Provider certain Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **SDPA Definitions.** The definition of terms used in this SDPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this SDPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement and any terms of service or privacy policies of Provider.

Article II. ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of LEA. Provider further acknowledges and agrees that all copies of such Student Data transmitted to Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this SDPA 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 LEA. For the purposes of FERPA, Provider shall be considered a School Official, under the control and direction of LEA as it pertains to the use of Student Data, notwithstanding the above. This provision shall not be interpreted as enabling the LEA to assert any intellectual property right over the products or services provided to the LEA by the Provider pursuant to the Service Agreement.
2. **Parent Access.** To the extent required by law, LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and Student Data and 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 (but no later than forty-five (45) days from the date of the request or the time frame required under state law for LEA to respond to a parent or student, whichever is sooner) to LEA's request for Student Data in a student's records held by Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts Provider to review any of the Student Data accessed pursuant to the Services, Provider shall refer the parent or individual to 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 Provider, then Provider shall, at the request of LEA, transfer, or provide a mechanism for 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 (each a "Requesting Party") contact Provider with a request for Student Data held by Provider pursuant to the SDPA Services, Provider shall notify LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform LEA of the request.
5. **Subprocessors.** Provider shall enter into written Agreements with all Subprocessors performing functions for Provider in order for Provider to provide the Services (as defined in the Service Agreement), whereby each Subprocessor agrees to protect Student Data in a manner no less stringent than the terms of this SDPA.

Article III. ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the SDPA 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 LEA has a policy of disclosing Education Records or Student Data under FERPA (34 CFR § 99.31(a)(1)), then 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 SDPA 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. ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** 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 SDPA Services outlined in Exhibit "A", or stated in the Service Agreement, or otherwise authorized under the statutes referred herein.

account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this SDPA and its accompanying exhibits.

Article V. **ARTICLE V: DATA PROVISIONS**

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of 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 LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, Provider shall allow 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 LEA. Provider will cooperate reasonably with LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of Provider or delivery of SDPA Services to students or LEA, and shall provide reasonable access to Provider's facilities, staff, agents, and Student Data and all records pertaining to Provider, LEA, and delivery of SDPA Services to LEA. Failure by Provider to reasonably cooperate as described herein shall be deemed a material breach of this SDPA. All costs related to the audit, including any cost incurred by the Provider in relation to its cooperation with the audit, shall be paid by LEA in advance.
3. **Data Security.** Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. Provider shall adhere to any applicable law relating to data security. Provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an addendum to **Exhibit "F"**. 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 designate an employee to serve as LEA's primary contact regarding 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 Provider, Provider shall notify LEA in writing within seventy-two (72) hours of confirmation of the incident unless the timing of such notification 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 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. 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
 - iv. 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 SDPA Services, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

Article VI. **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 SDPA, they may do so by mutual written consent so long as the Service Agreement has expired or has been terminated. Either party may terminate this SDPA and any service Agreement or contract if the other party breaches any terms of this SDPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, then Provider shall destroy all Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This SDPA 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 SDPA. In the event there is conflict between the terms of this SDPA and the Service Agreement, any terms of service or privacy policies or Provider, or with any other bid/RFP, license Agreement, or writing, the terms of this SDPA shall control. In the event of a conflict between **Attachment “_”**, the SDPC Standard Clauses, and the Supplemental State Terms, **Attachment “_”** will control, followed by the Supplemental State Terms. Except as described in this paragraph, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This SDPA 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 SDPA may be amended and the observance of any provision of this SDPA 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 SDPA 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 SDPA, 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, then it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this SDPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS SDPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF FLORIDA, 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 LAKE COUNTY, FLORIDA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SDPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound.** This SDPA 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 Provider sells, merges, or otherwise disposes of its business to a successor during the term of this SDPA, Provider shall provide written notice to 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 SDPA and any obligations with respect to Student Data within the Service Agreement. LEA has the authority to terminate the SDPA if it disapproves of the successor to whom Provider sells, merges, or otherwise disposes of its business.

8. **Authority.** Each person signing this SDPA hereby represents that he or she is fully authorized to legally and effectively bind to the terms of this SDPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, the party they purport to represent and all related or associated institutions, individuals, employees or providers who may have access to the Student Data 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

Please describe the functionality of the product and include if the application is a subscription or free online service. Also, include if the data is stored exclusively in the United States. If not, then list the countries in which data is stored.

EXHIBIT B
SCHEDULE OF DATA [Digital Passport/Compass/Connection]

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	Yes
	Other application technology meta data-Please specify:	See "Other" section
Application Use Statistics	Meta data on user interaction with application	Yes
Assessment	Standardized test scores	No
	Observation data	No
	Other assessment data-Please specify:	No
Attendance	Student school (daily) attendance data	No
	Student class attendance data	No
Communications	Online communications captured (emails, blog entries)	No
Conduct	Conduct or behavioral data	No
Demographics	Date of Birth	No
	Place of Birth	No
	Gender	No
	Ethnicity or race	No
	Language information (native, or primary language spoken by student)	No
	Other demographic information-Please specify:	n/a
Enrollment	Student school enrollment	No
	Student grade level	No
	Homeroom	No
	Guidance counselor	No
	Specific curriculum programs	No
	Year of graduation	No
	Other enrollment information-Please specify:	No
Parent/Guardian Contact Information	Address	No
	Email	No
	Phone	No

Parent/Guardian ID	Parent ID number (created to link parents to students)	No
Parent/Guardian Name	First and/or Last	No
Schedule	Student scheduled courses	No
	Teacher names	No
Special Indicator	English language learner information	No
	Low income status	No
	Medical alerts/ health data	No
	Student disability information	No
	Specialized education services (IEP or 504)	No
	Living situations (homeless/foster care)	No
	Other indicator information-Please specify:	No
Student Contact Information	Address	No
	Email	No
	Phone	No
Student Identifiers	Local (School district) ID number	No
	State ID number	No
	Provider/App assigned student ID number	No
	Student app username	No
	Student app passwords	No
Student Name	First and/or Last	No
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	No
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	No
Student Survey Responses	Student responses to surveys or questionnaires	No
Student work	Student generated content; writing, pictures, etc.	No
	Other student work data -Please specify:	No
Transcript	Student course grades	No
	Student course data	No
	Student course grades/ performance scores	No
	Other transcript data - Please specify:	No
Transportation	Student bus assignment	No
	Student pick up and/or drop off location	No

	Student bus card ID number	No
	Other transportation data – Please specify:	No
Other	<p>Please list each additional data element used, stored, or collected by your application:</p> <p><u>Children's Information.</u> The product is used anonymously. Players enter a short user name to begin. If users choose to save a game, they can use this name to resume play, but this is stored locally and is not collected by or accessible to Common Sense. If directed by teachers, users may choose to print or save a copy of the scorecard which displays any entered user name. Common Sense does not collect such files.</p> <p><u>Information Collected Through Technology.</u> If a user wishes to save a game, we enable cookies so as to remember the user's progress. Through these cookies, Common Sense and its service providers may collect certain non-personal information automatically when the service is used. Such information may include anonymous information about the use of the Service, device type (e.g., iPad Air), browser, operating system (e.g., iOS 12.4), and country, state, and city. We use this information to administer and improve the user's experience on our Service, to help diagnose and troubleshoot potential server malfunctions, and to gather broad demographic information. Common Sense uses Google Analytics to collect and aggregate this information, which is not able to track a user across devices, apps, or sites.</p> <p><u>Information Retained on Device or in Browser.</u> If a user wishes to save a game, the game will store username and score data for a player. This information is stored locally in a browser, and is not collected by Common Sense or accessible to Common Sense. This information persists until a user deletes it by clearing the browser cache.</p> <p><u>NOTE on cookie information.</u> Users make a choice at the first start of play whether they wish to save a game and enable cookies. If cookies are enabled, information is collected as described above. To <u>learn more</u> about the use of cookies see the privacy notices for the products at: https://www.digitalpassport.org/privacy.html https://www.digitalpassport.org/privacy.html</p>	

None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	n/a

EXHIBIT "B"

SCHEDULE OF DATA [Google Quizzes]

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	Yes
	Other application technology meta data-Please specify:	See "Other" section
Application Use Statistics	Meta data on user interaction with application	Yes
Assessment	Standardized test scores	No
	Observation data	No
	Other assessment data-Please specify:	See "Other" Section
Attendance	Student school (daily) attendance data	No
	Student class attendance data	No
Communications	Online communications captured (emails, blog entries)	No
Conduct	Conduct or behavioral data	No
Demographics	Date of Birth	No
	Place of Birth	No
	Gender	No
	Ethnicity or race	No
	Language information (native, or primary language spoken by student)	No
	Other demographic information-Please specify:	n/a
Enrollment	Student school enrollment	No
	Student grade level	No
	Homeroom	No
	Guidance counselor	No
	Specific curriculum programs	No
	Year of graduation	No
	Other enrollment information-Please specify:	No
Parent/Guardian Contact Information	Address	No
	Email	No
	Phone	No

Parent/Guardian ID	Parent ID number (created to link parents to students)	No
Parent/Guardian Name	First and/or Last	No
Schedule	Student scheduled courses	No
	Teacher names	No
Special Indicator	English language learner information	No
	Low income status	No
	Medical alerts/ health data	No
	Student disability information	No
	Specialized education services (IEP or 504)	No
	Living situations (homeless/foster care)	No
	Other indicator information-Please specify:	
Student Contact Information	Address	No
	Email	No
	Phone	No
Student Identifiers	Local (School district) ID number	No
	State ID number	No
	Provider/App assigned student ID number	No
	Student app username	No
	Student app passwords	No
Student Name	First and/or Last	No
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	No
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	No
Student Survey Responses	Student responses to surveys or questionnaires	No
Student work	Student generated content; writing, pictures, etc.	No
	Other student work data -Please specify:	No
Transcript	Student course grades	No
	Student course data	No
	Student course grades/ performance scores	No
	Other transcript data - Please specify:	No
Transportation	Student bus assignment	No
	Student pick up and/or drop off location	No
	Student bus card ID number	No
	Other transportation data – Please specify:	n/a

Other	<p>Please list each additional data element used, stored, or collected by your application:</p> <p>The Digital Citizenship Curriculum offers an interactive quiz for every lesson in grades 3–12. Every quiz features five questions that can help teachers assess students' mastery of core digital citizenship concepts and dispositions. The quiz tool is integrated with the Google Classroom platform and Google API for user authentication. By using the school Google accounts, teachers don't need to make quiz accounts for your classes of students.</p> <p>In order to assign quizzes to students with Google Classroom, teachers need to allow Common Sense Education access to certain permissions on the Google account used with Google Classroom. If the permissions are granted, Common Sense Media will have limited access to certain information as described in this Exhibit. For additional information see:</p> <ul style="list-style-type: none"> - Lesson Quiz Guide at - FAQ page at https://commonsense.force.com/membersupport/s/topic/0TO1R000001Ft3fWAC/digital-citizenship-lesson-quizzes 	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	n/a

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 SDPA in its entirety with Provider.

Provider: For purposes of the SDPA, 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 SDPA 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 SDPA and pursuant to 34 CFR § 99.31(b), a School Official is a Provider 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 Agreement for Online Educational Services between Provider and LEA and any purchase orders, terms of service, or terms of use related to the products or services to be provided or performed thereunder.

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 SDPA, 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 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 SDPA, the term "Subprocessor" (sometimes referred to as "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate 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 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 SDPA, the term "Third Party" when used to indicate Provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT D
DIRECTIVE FOR DISPOSITION OF DATA

LEA hereby directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider as follows:

1. Extent of Disposition- Disposition extends to all categories of data
2. Nature of Disposition- Disposition shall be by full and complete destruction or deletion of data. Provider shall provide written confirmation to LEA confirming the date and nature of data destruction.
3. Schedule of Disposition- Data shall be disposed of no later than thirty (30) days after the expiration or earlier termination of the Service Agreement.

(Exhibit – No Signature Required)

Name: _____

As: Authorized Representative of LEA

Date: _____

By signing below, I hereby acknowledge receipt of this Directive for Disposition of Data on behalf of Provider.

(Exhibit – No Signature Required)

Name: _____

As: Authorized Representative of LEA


Date: _____

EXHIBIT E
GENERAL OFFER OF TERMS

OFFER OF TERMS:

Provider offers the same privacy protections found in this SDPA between it and The School Board of Lake County, Florida ("**Originating LEA**") which is dated [**Insert Date**], to any other local education agency ("**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 SDPA. Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to Provider to suit the unique needs of the Subscribing LEA. 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 LEA's Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEA should send the signed **Exhibit "E"** to Provider at the following email address:

PROVIDER NAME: Common Sense Media

Signature: 

Date: 06 / 15 / 2023

Printed Name: David Kuizenga

Title/Position: Chief Financial & Administrative Officer

ACCEPTANCE BY SUBSCRIBING LEA:

Subscribing LEA, by signing a separate service agreement with Provider, and by its signature below, hereby accepts the General Offer of Privacy Terms. Subscribing LEA and Provider shall therefore be bound by the same terms of this SDPA for the term of this SDPA between The School Board of Lake County, Florida and Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

SUBSCRIBING LEA NAME: _____

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

SUBSCRIBING LEA'S DESIGNATED REPRESENTATIVE:

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)	NIST Cybersecurity Framework Version 1.1
National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
International Standards Organization (ISO)	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)	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 FLORIDA

Version _____

None

EXHIBIT H
ADDITIONAL TERMS OR MODIFICATIONS

1. The second WHEREAS CLAUSE is hereby amended to add “, and the Protection of Pupil Rights Amendment (“PPRA”) at 20 U.S.C. 1232h (34 CFR Part 98)” after “15 U.S.C. § 6501-6506 (16 CFR Part 312)”.
2. Paragraph 3 on the first page of the SDPA is hereby deleted in its entirety and replaced with the following:

In the event of a conflict between the SDPA Standard Clauses, the Special Provisions will control. In the event there is conflict between the terms of the SDPA and any other writing, including any terms of service or privacy policy of Provider, the terms of the Service Agreement shall control, and any remaining conflicts will be controlled by the terms of this SDPA.

or Subprocessor(s) related to Attachment A, Exhibit B (Schedule of Data), including but not limited to, failure to notify School Board of any additional students’ PII collected and not updated by Provider in Exhibit B.

3. Article II, Paragraph 5 is hereby deleted in its entirety and replaced with the following:

Provider shall enter into written Agreements with all Subprocessors performing functions for Provider in order for Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this SDPA. Provider agrees to share the Subprocessors names and Agreements with LEA upon LEA’s request.

4. Article III, Paragraph 1 is hereby amended to add the following sentence:

LEA will allow Provider access to Student Data necessary to perform the Services and pursuant to the terms of this SDPA and in compliance with FERPA, COPPA, PPRA, and all other privacy statutes cited in this SDPA.

5. Article IV, Paragraph 1 is hereby amended to add the following sentence:

The Parties expect and anticipate that Provider may receive personally identifiable information in

education records from the District only as an incident of service or training that Provider provides to LEA pursuant to this Agreement. Provider shall comply with all applicable State and Federal laws and regulations pertaining to Student Data privacy and security, including FERPA, COPPA, PPR, Florida Statutes Sections 1001.41 and 1002.22, and all other privacy statutes cited in this SDPA. The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records because for purposes of the contract, Provider: (1) provides a service or function for which LEA would otherwise use employees; (2) is under the direct control of LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records

6. Article IV, Paragraph 2 is hereby amended to add the following sentence:

Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta Student Data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of LEA.

7. Article IV, Paragraph 7 is hereby deleted in its entirety and replaced with the following:

8. Article V, Paragraph 1 is hereby deleted in its entirety and replaced with the following:

Student Data shall be stored within the United States. Upon request of LEA, Provider will provide a list of the locations where Student Data is stored. Provider shall not, without the express prior written consent of District: Transmit Student Data or PII to any Providers or Subprocessors located outside of the United States; distribute, repurpose or share Student Data or PII with any Partner Systems not used for providing services to LEA; use PII or any portion thereof to inform, influence or guide marketing or advertising efforts, or to develop a profile of a student or group of students for any commercial purpose [or for any other purposes]; use PII or any portion thereof to develop commercial products or services; use any PII for any other purpose other than in connection with the services provided to LEA; and engage in targeted advertising, based on the Student Data collected from LEA.

9. Article VII, is hereby amended to add Paragraph 10 as follows:

Assignment. None of the Parties to this SDPA may assign their rights, duties, or obligations under this SDPA, either in whole or in part, without the prior written consent of the other party to this SDPA.

10. Article VII, is hereby amended to add Paragraph 11 as follows:

Click through. Any "click through" terms and conditions or terms of use are superseded by the Service Agreement and this SDPA, and acceptance of the terms and conditions or terms of use through the "click through" do not indicate acceptance by the entity.

11. Article VII, is hereby amended to add Paragraph 12 as follows:

Security Controls. Security Controls. Provider represents and warrants that any software licensed hereunder shall not contain any virus, worm, Trojan Horse, tracking software or be capable of identifying non-approved users or tracking any approved user, or any undocumented software locks or drop dead devices that would render inaccessible or impair in any way the operation of the software or any other hardware, software or data for which the software is designed to work with.

Title	Common Sense Media DPA
File name	Common Sense Media.pdf
Document ID	324d1c54f14b87eafeac0cfae6e06ac43aeafa80
Audit trail date format	MM / DD / YYYY
Status	• Signed

Document History



SENT

06 / 15 / 2023
12:34:45 UTC-4

Sent for signature to David Kuizenga
(dkuizenga@commonsense.org) from aronsk@lake.k12.fl.us
IP: 150.176.175.200



VIEWED

06 / 15 / 2023
17:58:16 UTC-4

Viewed by David Kuizenga (dkuizenga@commonsense.org)
IP: 73.47.248.220



SIGNED

06 / 15 / 2023
17:59:13 UTC-4

Signed by David Kuizenga (dkuizenga@commonsense.org)
IP: 73.47.248.220



COMPLETED

06 / 15 / 2023
17:59:13 UTC-4

The document has been completed.