WASHINGTON STUDENT DATA PRIVACY AGREEMENT

Version 1.0

TACOMA PUBLIC SCHOOLS

and

CODE.ORG

This Washington Student Data Privacy Agreement ("DPA") is entered into by and between the Tacoma Public Schools (hereinafter referred to as "LEA") and Code.org (hereinafter referred to as "Provider") on ______________. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain

digital educational services ("Services") pursuant to Code.org terms of service located at https://code.org/tos ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. § 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several Washington State privacy laws, including Student User Privacy in Education Rights ("SUPER") 28A.604.010 *et seq*., as well as RCW 19.255.010 *et seq.* and RCW 42.56.590.

WHEREAS, for the purposes of this DPA, Provider is a School Official with legitimate educational interests in accessing educational records and performing Services pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in Washington the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

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

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 transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SUPER and other applicable Washington State laws, 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. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA. This DPA, together with the Service Agreement, is the "Agreement".

2. **Nature of Services Provided**. The Provider has agreed to provide the digital educational products and Services outlined in Exhibit "A" attached hereto and any other products and services that Provider may provide now or in the future (the "Services").

3. **Student Data to Be Provided**. In order to perform the Services described in the Service Agreement, LEA shall provide the categories of Student Data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B":

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C" attached hereto. In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

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.

2. **Exemptions under** FERPA For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer student-generated content to a separate account, according to the procedures set forth below.

3. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the student's records, 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 timely manner (and no later than 45 days from the date of the request) 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.

4. **Separate Account**. If Student Generated Content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider may, at the request of the parent or eligible student, transfer said Student Generated Content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Services.

4. **Third Party Request**. Should a Third Party, excluding a Subprocessor, including law enforcement 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 Student 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.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance** LEA shall provide data to Provider for the purposes of the Service Agreement in compliance with any applicable state or federal laws and regulations pertaining to data privacy and security, including, without limitation, FERPA, COPPA, PPRA, SUPER and all other Washington privacy statutes.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under 4 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.

If LEA is providing Directory Information or any Education Record to Provider, LEA represents, warrants and covenants to Provider, as applicable, that LEA has:

(i) 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

(ii) 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

(iii) 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.

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. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to its computer systems, Services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly 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 access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, applicable to Provider providing the Service to LEA including, COPPA, , SUPER and all other Washington privacy statutes. 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.

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 stated in the Service Agreement and/or otherwise legally permissible, including without limitation, for adaptive learning or customized student learning. The foregoing limitation does not apply to any De-Identified Data.

3. **Employee Obligation**. Provider shall require all officers, employees and agents (including, but not limited to, Subprocessors) 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.

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 2.4 ; (vi) to protect the safety or integrity of users or others, or the security of the Services; or (vii) to Subprocessors, in connection with operating or improving the Service. Provider will not Sell (as defined in Exhibit C) Student Data.

5. **De-identified Data.** De-identified Data may be used by the Provider for any lawful purpose, including, without limitation, the purposes of 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 Student Data and not to transfer de-identified Student Data to any party unless that party agrees in writing not to attempt re-identification,.

5. **Disposal of Data**. Upon a written request from the LEA, Provider shall dispose of or delete all Student Data obtained under the Service Agreement within thirty (30) days of the date of the receipt of such 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. Disposal shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing any Personally Identifiable Information; or (3) Otherwise modifying the Personally Identifiable Information in those records to make it unreadable and/or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposal, unless a student, parent or legal guardian of a student chooses to establish a personal login to their account. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is

attached hereto as Exhibit "D"). Upon receipt of a request from the LEA, the Provider will provide the LEA with any specified portion of the Student Data within thirty (30) calendar days of receipt of said request.

a. **Partial Disposal During Term of Service Agreement.** Throughout the term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA's or a parent's request to transfer data to a Student Generated Content account pursuant to Article II, section 3, above. The LEA may also request that specific Student Data be returned to the LEA.

b. **Complete Disposal Upon Termination of Service Agreement.** Upon termination of the Service Agreement Provider shall dispose of or delete all Student Data obtained under the Service Agreement. Prior to disposal of the data, Provider shall notify LEA of its option to transfer data to a Student Generated Content account pursuant to Article II, section 3, above, or to other accounts as may be designated by the LEA. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

c. **Pre-termination Data Disposal Meeting.** In addition to the foregoing requirements, the LEA may request in writing that Provider participate in a meeting to discuss disposal of the Student Data prior to termination of the Service Agreement.

6. Advertising Prohibition. Provider is prohibited from using or selling Student Data to (a) serve Targeted Advertising to students or families/guardians unless with the consent of the parent or legal guardian or LEA; (b) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA or as authorized by the parent or legal guardian or LEA; or (c) use the Student Data for the development of commercial products or Services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes, or from (i) 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; (ii) apply to the marketing of school memorabilia such as photographs, yearbooks, or class rings, (iii) prohibit Provider from using aggregate or De-Identified Data to inform, influence or enable marketing, advertising or other commercial efforts by Provider, (iv) limit the ability of Provider to use Student Data for adaptive learning or customized student learning purposes , (v) prohibit Provider from using Student Data to recommend educational products or services to parents/guardians, students, or LEAs so long as the recommendations are not based in whole or part by payment or other consideration from a third party, (vi) 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 .

ARTICLE V: DATA SECURITY AND BREACH PROVISIONS

1. **Data Security**. The Provider agrees to employ administrative, physical, and technical safeguards, consistent with industry standards and technology best practices, to protect Student Data from unauthorized use, access, disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" attached 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 suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees, contractors and/or Subprocessors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

b. Destruction of Data. Provider shall destroy or delete all Student Data obtained under the Service Agreement according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposal work authorized under the Service Agreement.

c. Security Protocols. Both parties agree to maintain security protocols that meet industry standards 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 Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA or as set forth in the Agreement. The foregoing does not limit the ability of the Provider to allow any necessary Subprocessors to view or access data as set forth in Article IV, Section 4.

d. Employee Training. The Provider shall provide periodic security training to those of its employees who operate or who are authorized to access the Provider's computer systems and/or the Student Data. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

f. Mobile Use of Student Data. Provider shall ensure that any and all mobile devices of any type (including, but not limited to, laptops, tablets, and phones), which are used for access to, storage or analysis of Student Data by Provider's employees and/or contractors shall be protected by industry standard encryption to prevent unauthorized access by third parties. Provider shall also implement a Bring Your Own Device ("BYOD") policy for its own employees, which requires them to use physical and technical safeguards against third party access to the device, and a copy of that BYOD policy shall be provided to LEA as part of Exhibit F to this DPA.

g. **Security Technology**. When the Student Data is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host Student Data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

h. **Security Coordinator**. If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

i. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V.

j. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

k. **Compliance Audit.** LEA shall have the right but shall be under no obligation to conduct audit(s), from time to time, of Provider's records concerning its compliance obligations as set forth in this Article V. Provider shall make such records and other documents available to LEA upon receipt of a written request from the LEA with at least ten (10) business day notice, the Provider will allow the LEA to audit, during normal business hours and at a time convenient for Provider, the security and privacy measures that are in place to ensure protection of the Student Data or any portion thereof ("Security Audit"). LEA may not request more than one Security Audit per year, except in the case of a verified breach. Notwithstanding the forgoing, the parties agree that the LEA and any local, state, or federal agency with oversight authority/jurisdiction may conduct an audit at any time, in the event an audit is required by governmental or regulatory authorities ("Regulatory Audits"). In connection with any Regulatory Audit or Security Audit, of the Provider , Provider will provide 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 as needed to fulfill the requests of such Regulatory or Security Audit.. Failure to cooperate in good faith shall be deemed a material breach of the Agreement. Costs for the audit are the responsibility of the LEA.

2. Data Breach. In the event that Provider becomes aware of any actual or reasonably suspected unauthorized disclosure of or access to any Student Data covered by this Agreement ("Security Incident"), Provider shall provide notification to LEA as required by the applicable state law following discovery of the Security Incident (each a "Security Breach Notification"). Unless otherwise required by the applicable law, the Security Breach Notification shall contain the following:

a. The Security Breach 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 Breach Notification described above in section 2(a) shall include, at a minimum, the following information:

i. The name and contact information of the reporting Provider subject to this section.

ii. A list of the types of Student Data that were or are reasonably believed to have been the subject of the Security Incident.

iii. 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 notification shall also include the date of the notice.

iv. Whether, to the knowledge of the Provider, the Security Breach Notification was delayed as a result of a law enforcement investigation and the law enforcement agency determined that notification would impede a criminal investigation.

v. A general description of the breach Security Incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the Security Breach Notification may also include any of the following:

i. Information about what the Provider has done to protect individuals whose PII has been breached by the Security Incident.

ii. Advice on steps that the person whose PII has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements applicable to Provider in state and federal law 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.

e. Provider further acknowledges and agrees to have a written incident response plan that is consistent with industry standards and federal and state law applicable to Provider for responding to a Security Incident of Student Data or any portion thereof, including Personally Identifiable Information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

f. Except as otherwise required by law, Provider is prohibited from directly contacting parent, legal guardian or eligible student unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible student of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

g. In the event of a Security Incident originating from LEA's actions, use or misuse of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI – INDEMNITY

1. Indemnity. Provider shall defend, indemnify and hold harmless the LEA, its officers, directors, employees, agents and assigns (the "Indemnitees") from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance carrier (the "Claims"), arising out of or resulting from any third-party claim against the Indemnitees arising out of or resulting from Provider's failure to comply with any of its obligations under this DPA. Provider's duty to defend and indemnify the LEA includes any and all claims and causes of action whether based in tort, contract, statute, or equity. LEA agrees not to settle any matter without the prior written consent of Provider. LEA will use reasonable efforts to notify Provider of any such Claims upon becoming aware of it.

Provider's defense and indemnity obligations herein are intended to provide for the broadest indemnity rights available under Washington law and shall survive the termination of this DPA. To the extent

Provider’s defense and indemnity obligations as set forth in this DPA conflict with the terms of the Service Agreement, the defense and indemnity provisions set forth herein shall control.

ARTICLE VII- GENERAL OFFER OF PRIVACY 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 this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VIII: MISCELLANEOUS

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

2. **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 shall have the right to terminate the DPA and Service Agreement in the event of a material breach by the other Party, its employees, or agents of the terms of this DPA.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA’s Student Data pursuant to Article V, section 1(b), and Article II, section 3, above.

4. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. With respect to Student Data in the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. No indemnification provisions granted bythe LEA in the Service Agreement shall be effective as to a breach of the terms of this DPA by the Provider. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this DPA is:

Name:
Title:

Contact Information:

____
____
____

The designated representative for the Provider for this DPA is:

Name:
Title: Privacy Officer

Contact Information: privacy@code.org
Code.org, attn: Privacy
1501 4th Ave, Ste 900
Seattle, WA 98101

b. Notification of Acceptance of General Offer of Terms. Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: Alex Brenner
Title: Director of Accounting & Finance

Contact Information: privacy@code.org
Code.org, attn: Privacy
1501 4th Ave, Ste 900
Seattle, WA 98101

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.

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.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF WASHINGTON, 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 IN WHICH THE LEA IS LOCATED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Both Parties represent that they are 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

10. **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.

11. **Successors Bound**. This DPA is and shall be binding upon Provider’s respective successors in interest 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.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this Washington Student Data Privacy Agreement as of the last day noted below.

Name of Provider: Code.org

BY: Date: 8·29·19

Printed Name: Alice Steinglass Title/Position: President

Address for Notice Purposes:

Name of Local Education Agency: Tacoma Public Schools

BY: Edward Grassia Date: 8/30/19

Printed Name: Edward Grassia Title/Position: Chief Information Officer

Address for Notice Purposes:

Central Administration Building P.O. Box 1357 Tacoma, WA 98401-1357

Note: Electronic signature not permitted.

IN WITNESS WHEREOF, the parties have executed this Washington Student Data Privacy Agreement as of the last day noted below.

Name of Provider: Code.org

BY: Date:

Printed Name: Title/Position:

Address for Notice Purposes:

Name of Local Education Agency: Tacoma Public Schools

BY: Date:

Printed Name: Title/Position:

Address for Notice Purposes:

Note: Electronic signature not permitted.

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	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	

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)	
	Living situations (homeless/foster care)	
	Other indicator information- Please specify:	
Student Contact Information	Address	
	Email (used temporarily to recover an account, not stored)	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	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)	X
Student Program Membership	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 etc.	X

Category of Data	Elements	Check if used by your system
(Other)	Other student work data - Please specify: Projects and Code.org coursework	X
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	

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

EXHIBIT "C"

DEFINITIONS

ACPE (Association for Computer Professionals in Education): Refers to the membership organization serving educational IT professionals in the States of Oregon and Washington to promote general recognition of the role of IT professionals in educational institutions; improve network and computer services; integrate emerging technologies; encourage appropriate use of information technology for the improvement of education and support standards whereby common interchanges of electronic information can be accomplished efficiently and effectively.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the 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 as identified by Washington Compact Provision 28A.705.010.. For purposes of this DPA, Educational Records are referred to as Student Data.

De-Identifiable Information (DII) or De-Identified Data: De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from Student Data in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Indirect Identifiers: Indirect identifiers include information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator (*e.g.*, state, county) and other descriptors.

NIST: Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

Operator: The term "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 primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Data Privacy Agreement, the term "Operator" is replaced by the term "Provider.".

Persistent Unique Identifiers. A long-lasting identification for digital objects, which allows for those digital objects to be located even if they are moved or removed. Persistent identifiers that are not anonymized, De-Identified or aggregated are personal information.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" means data 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.. PII includes Indirect Identifiers For purposes of this DPA, Student Personally Identifiable Information shall include the categories of information listed in the definition of PII under FERPA.

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or Services, including cloud-based services, for the digital storage, management, and retrieval of student records. Within the DPA the term "Provider" includes the term "Operator" as used in applicable state statutes.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, and Student Personal Information, all of which are deemed Student Data for the purposes of this Agreement.

Sell: Consistent with the 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.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to FERPA (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 education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from Educational Records.

Student Data: Student Data includes any Personally Identifiable Information, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians through a school service or 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 identities, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of federal 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 Data, or anonymous usage data regarding a student's use of Provider's Services.

Student Generated Content: The term "Student Generated Content" means materials or content created by a student during and for the purpose of education 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.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

Subprocessor: For the purposes of this Agreement, 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 software, and who has access to Student Data.

Targeted Advertising: 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. This 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 website or a response to a student's response or request for information or feedback, both of which are permitted. Targeted Advertising also does not include adaptive learning, personalized learning, or customized education.

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 student records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS
TACOMA PUBLIC SCHOOLS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Tacoma Public Schools and which is date ________ to any other LEA ("Subscribing LEA") who accepts this General Offer though 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 other LEA may also agree to change the data provided by LEA to the Provider to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the Services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify ACPE in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

BY: ______________________________ Date: 8·29·19

Printed Name: Alice Steinglass Title/Position: President

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.

BY: Date:

Printed Name: Title/Position

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW

Name: Alex Brenner

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS
TACOMA PUBLIC SCHOOLS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Tacoma Public Schools and which is date ________ to any other LEA ("Subscribing LEA") who accepts this General Offer though 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 other LEA may also agree to change the data provided by LEA to the Provider to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the Services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify ACPE in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

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.

BY: Date:

Printed Name: Title/Position

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW

Name: Alex Brenner

Title: Director of Finance & Accounting

Email Address: privacy@code.org

EXHIBIT “F”

DATA SECURITY REQUIREMENTS