DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

STUDENT DATA PRIVACY ADDENDUM[1]

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

RECITALS

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

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

WHEREAS, the documents and data transferred from LEAs and created or accessed by the Provider's Services are also subject to various state student privacy laws, including, but not limited to, New York State Education Law § 2-d ("Education Law §2-d"); and

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

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

1. PURPOSE AND SCOPE

1.1. Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit "C") transmitted to Provider from the LEA and its users pursuant to the Service Agreement including compliance with all applicable federal and state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, and New York State Education Law 2-d. This DPA supplements the Service Agreement and together with the Service Agreement, is collectively referred to as the "Agreement".

1.2. Nature of Services Provided. Pursuant to and as fully described in the Service Agreement, Provider has agreed to provide the digital educational services as set forth in Exhibit "A" hereto and any other products and services that Provider may provide now or in the future (the "Services").

1.3. Student Data to Be Provided. In order to perform the Services, the Parties shall indicate the categories of Student Data to be provided or collected by the Provider in the Schedule of Data, attached hereto as Exhibit "B".

1.4. DPA Definitions. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, the Service Agreement, privacy policies or

[1] Modeled After The Student Data Privacy Consortium's Set Of Baseline Model Clauses

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

any terms of service with respect to the treatment of Student Data.

2. DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1. **Student Data Property of LEA.** All Student Data or any other Education Records (as defined on Exhibit "C" transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent). The Provider further acknowledges and agrees that all copies of such Student Data or Education Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Education Records. The Parties agree that as between them, all rights, including all intellectual property rights, in and to Student Data or Education Records covered per this Agreement shall remain the exclusive property of the LEA or the party who provided such data (such as the student or parent).

2.2. **Exemptions under FERPA.** LEA may not generally disclose Personally Identifiable Information from an eligible student's Education Record to a third-party without written consent of the parent and/or eligible student or without meeting one of the exemptions set forth in FERPA ("FERPA Exemption(s)"), including the exemption for Directory Information ("Directory Information Exemption") or School Official exemption ("School Official Exemption"). For the purposes of FERPA, to the extent Personally Identifiable Information from Education Records are transmitted to Provider from LEA or from students using accounts at the direction of the LEA, the Provider shall be considered a School Official as defined on Exhibit "C", under the control and direction of the LEAs as it pertains to the use of Education Records. Additionally, certain information, provided to Provider by LEA about a student, such as student name and grade level, may be considered Directory Information as defined on Exhibit "C" under FERPA and thus not an Education Record.

2.3. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information contained in the related student's Education Records and correct erroneous information, consistent with the functionality of Services. Provider shall cooperate and respond within thirty (30) days to the LEA's request for Personally Identifiable Information contained in the related student's Education Records held by the Provider to view or correct as necessary. In the event that a parent/legal guardian of a student, an eligible student or other individual contacts the Provider to review any of the Education Records or Student Data accessed pursuant to the Services, the Provider shall refer the parent, eligible student or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information, provided however, that Provider may also allow for direct access requests (but not correction or deletion rights) of Student Data and/or Education Records from a verified parent.

2.4. **Separate Accounts and Outside School Logins.** Students and parent users may have personal or non-school accounts (i.e. for use of Code.org at home not related to school) in addition to school accounts ("Outside School Accounts"). Additionally, they may choose to create personal login information to student accounts to continue developing projects or work outside of school ("Personal Login"). Student Data shall not include information a student or parent provides to Provider through such Outside School Account or use of a school account with a Personal Login independent of the student's or parent's engagement with the Services at the direction of the LEA. Additionally, If Student Generated Content is stored or maintained by the Provider as part of the Services, Provider may, at the request or with the consent of the parent or legal guardian, transfer said Student Generated Content to a separate student account or the Outside School

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

Account or continue to use such content within the former school account with a Personal Login upon termination of the Service Agreement; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service.

2.5. **Third Party Request.** Should a third party, excluding a Service Provider, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall redirect the third party to request the data directly from the LEA, unless and to the extent that Provider reasonably believes it must grant such access to the third party because the data disclosure is necessary: (i) pursuant to a court order or legal process, (ii) to comply with statutes or regulations, (iii) to enforce the Agreement, or (iv) if Provider believes in good faith that such disclosure is necessary to protect the rights, property or personal safety of Provider's users, employees or others. Provider shall notify the LEA in advance of a compelled disclosure to a third party, unless legally prohibited.

2.6. **Service Providers.** Provider shall enter into written agreements with all Service Providers performing functions pursuant to this Agreement, whereby the Service Providers agree to protect Student Data in manner no less stringent than the terms of this DPA. The list of Provider's current Service Providers can be accessed through the Provider's Privacy Policy (which may be updated from time to time).

3. DUTIES OF LEA

3.1. **Provide Data In Compliance With Laws.** LEA shall provide Student Data for the purposes of the Agreement in compliance with any applicable state or federal laws and regulations pertaining to data privacy and security, including, without limitation, the FERPA, PPRA, and IDEA. If LEA is providing Directory Information or any Education Record to Provider, LEA represents, warrants and covenants to Provider, as applicable, that LEA has:

a. complied with the Directory Information Exemption, including, without limitation, informing parents and eligible students what information the LEA deems to be Directory Information and may be disclosed and allowing parents and eligible students a reasonable amount of time to request that schools not disclose Directory Information about them; and/or

b. complied with the School Official Exemption, including, without limitation, informing parents in their annual notification of FERPA rights that the Institution defines "school official" to include service providers and defines "legitimate educational interest" to include services such as the type provided by Provider; or

c. obtained all necessary parental or eligible student written consent to share the Student Data with Provider, in each case, solely to enable Provider's operation of the Service.

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

3.2. **Reasonable Security.** LEA shall employ administrative, physical, and technical safeguards consistent with industry standards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted data from unauthorized access, disclosure or acquisition by an unauthorized person. In addition, LEA will align its data security practices to the NIST Cybersecurity Framework.

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

3.3. **Unauthorized Access Notification.** LEA shall notify Provider immediately, but in no less than 72 hours, of any known or suspected unauthorized use or access of the Services, LEA's account, or Student Data. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized use or access.

4. DUTIES OF PROVIDER

4.1. **Privacy Compliance.** The Provider shall comply in all material respects with all applicable state and federal laws and regulations pertaining to data privacy and security, applicable to the Provider in providing the Service to LEA. With respect to Student Data that the LEA permits Provider to collect or access pursuant to the Agreement, Provider agrees to support LEA in upholding LEA's responsibilities with FERPA and PPRA. Provider agrees that it will comply in all material respects with those provisions of the "LEA's Parent's Bill of Rights for Data Security and Privacy" ("Parents Bill of Rights"), a copy of which is attached hereto as Exhibit "F", that are applicable to Provider. Any terms not defined with the Parent's Bill of Rights shall have the meaning set forth in this DPA.

4.2. **Authorized Use.** Student Data shared pursuant to this Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services and for the uses set forth in the Agreement and/or as otherwise legally permissible, including, without limitation, for adaptive learning or customized student learning. The foregoing limitation does not apply to any De-Identified Data (as defined in Exhibit "C").

4.3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.

4.4. **No Disclosure.** Provider shall not disclose, transfer, share or rent any Student Data obtained under the Agreement in a manner that directly identifies an individual student to any other entity other than LEA, except: (i) as authorized by the Agreement; (ii) as directed by LEA; (iii) to authorized users of the Services, including parents or legal guardians; (iv) as permitted by law; (v) in response to a judicial order as set forth in Section 2.5; (vi) to protect the safety or integrity of users or others, or the security of the Services with prior written consent of the parent or eligible student; or (vii) to Service Providers, in connection with operating or improving the Service. Provider will not Sell (as defined in Exhibit "C") Student Data to any third party.

4.5. **De-Identified Data.** De-Identified Data may be used by the Provider for any lawful purpose, including, but not limited to, development, research, and improvement of educational sites, services, or applications, and to demonstrate the market effectiveness of the Services. Provider's use of such De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Provider agrees not to attempt to re-identify De-identified Data and not to transfer De-identified Data to any party unless that party agrees in writing not to attempt re-identification.

4.6. **Disposition of Data.** Provider shall, at LEA's request, dispose of or delete all Personally Identifiable Information contained in Student Data within a reasonable time period following a written request. If no written request is received, Provider shall dispose of or delete all Personally Identifiable Information contained in Student Data at the earliest of (a) when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law. Nothing in the DPA authorizes Provider to maintain Personally Identifiable Information contained in Student Data obtained under the Agreement beyond the time period reasonably needed to complete the disposition, unless

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

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

4.7. **Transfer of Student Data to LEA.** If a written request is received from LEA to transfer Personally Identifiable Information contained in Student Data to LEA, Provider shall transfer said Personally Identifiable Information contained in Student Data to LEA or LEA's designee within sixty (60) days of the date of such written request by LEA, or as required by law, and according to a schedule and procedure as the Parties may reasonably agree.

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

5. DATA SECURITY AND DATA BREACH

5.1. **Data Security.** The Provider agrees to employ administrative, physical, and technical safeguards consistent with industry standards designed to protect Student Data from unauthorized access, disclosure, use or acquisition by an unauthorized person, including when transmitting and storing such information. In addition, Provider will align its data security practices related to Student Data to the NIST Cybersecurity Framework. The general security duties of Provider are set forth below. Further detail regarding Provider's security programs and measures are set forth in Exhibit "E" hereto. Provider will not materially decrease the overall security of the Services during the term of the Agreement. These measures shall include, but are not limited to:

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

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

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

b. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data, including ensuring that Student Data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student Data obtained or generated pursuant to the Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Agreement except as necessary to provide the Service, to fulfill data requests by LEA or as otherwise set forth in the Agreement. The foregoing does not limit the ability of the Provider to disclose information as permitted under Section 2.5 or to allow any necessary Service Providers to view or access data as set forth in Section 4.4.

c. **Employee Training.** The Provider shall provide periodic security training to its officers, employees and contractors who operate or have access to the Services and Student Data ("Security Training"). The Security Training will include training on federal and state laws governing the confidentiality of Student Data prior to such officers, employees and contractors receiving access to Student Data.

d. **Security Technology.** When the Service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect Student Data from unauthorized access. The security measures employed shall include server authentication and data encryption at rest and in transit. Provider shall host Student Data pursuant to the Agreement in an environment using a firewall that is maintained according to industry standards.

e. **Security Coordinator.** The name and contact information of each Party's designated representative for the purposes of matters relating to security of Student Data received pursuant to the Agreement is set forth below:

i. Provider's security coordinator ("Security Coordinator") is: Bryan Djunaedi bryan@code.org.

ii. LEA's designated representative of matters relating to security of Student Data is set forth on the signature page of this DPA.

f. **Service Provider Bound**. Provider shall enter into written agreements whereby Service Providers agree to secure and protect Student Data in a manner no less stringent than the terms of this Section 5. Provider shall periodically conduct or review compliance monitoring and assessments of Service Providers to determine their compliance with this Section 5.

g. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

5.2. **Data Breach.** In the event that Provider becomes aware of any actual or reasonably suspected breach of security resulting in an unauthorized release or disclosure of or access to Student Data by Provider or its assignees in violation of applicable state of federal law, the Parents Bill of Rights, or the data privacy and security policies of the LEA (a "Security Incident"), Provider shall provide notification to LEA as required by the applicable state law, and in the most expedient way possible and without unreasonable delay, but in no event later than seven (7) calendar days of the incident

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

(each a "Security Incident Notification").The LEA shall, upon notification by the Provider, be required to report to the Chief Privacy Officer, who is appointed by the State Education Department, any such breach of security and unauthorized release of such data. Provider shall follow the following process:

a. Unless otherwise required by the applicable law, the Security Incident Notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The Security Incident Notification described above in Section 5.2(a) shall include such information required by the applicable state law, and at a minimum, the following information, to the extent available:

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

ii A list of the types of Personal Identifiable Information 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 Security Incident Notification shall also include the date of the notice.

iv Whether, to the knowledge of Provider at the time the Security Incident Notice was provided the notification was delayed as a result of a law enforcement investigation

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

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

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

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

d. Provider agrees to adhere to all requirements applicable to Provider providing the Service in applicable State and federal law with respect to a Security Incident related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such Security Incident.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a Security Incident involving Student Data or any portion thereof, including Personally Identifiable Information ("Incident Response Plan") and agrees to provide LEA, upon request, with a copy of the Incident Response Plan or a summary of such Incident Response Plan to the extent such plan includes sensitive or confidential information of Provider.

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

f. To the extent LEA determines that the Security Incident triggers third party notice requirements under applicable laws, Provider will cooperate with LEA as to the timing and content of the notices to be sent. Except as otherwise required by law, Provider will not provide notice of the Security Incident directly to individuals whose Personally Identifiable Information was affected, to regulatory agencies, or to other entities, without first providing written notice to LEA. This provision shall not restrict Provider's ability to provide separate security breach notification to customers, including parents and other individuals with Outside School Accounts.

g. Education Law 2-d additional requirements regarding Security Incident Notifications:

i In the case of a Security Incident involving Student Data, the LEA shall notify the parent or eligible student of the unauthorized release of Student Data that includes Personally Identifiable Information from the student records of such student in the most expedient way possible and without unreasonable delay.

ii In the case of notification to a parent or eligible student, due to a Security Incident involving Student Data by the Provider, or its Service Providers or assignees, and such Security Incident is not originating from LEA's use of the Service or otherwise a result of the LEA's actions or inactions, the Provider, if requested by the LEA and provided that Provider has not previously notified the affected parties, shall promptly reimburse LEA for the full cost of such notification, as required by Education Law §2-d(6)(c).

6. EDUCATION LAW 2-D SUPPLEMENTAL INFORMATION

6.1. In accordance with Education Law §2-d(3)(c) and Section 121.3 of the implementing Regulations, the attached Exhibit "G" includes the "Supplemental Information" required to be posted on the LEA's website.

7. MISCELLANEOUS

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

7.2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by terminating the Service Agreement as set forth therein. The LEA or Provider may terminate this DPA and the Service Agreement in the event of a material breach of the terms of this DPA.

7.3. **Effect of Termination Survival.** If the Service Agreement is terminated (thereby terminating this DPA), the Provider shall dispose of all of LEA's Personally Identifiable Information contained in Student Data following the procedures set forth in Section 4.6, which includes De-Identification.

7.4. **Priority of Agreements.** This DPA shall govern the treatment of Student Data. With respect to the treatment of Student Data, in the event there is conflict between the terms of the DPA, the Service Agreement, or any other agreement between Provider and LEA, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement, or any other agreement shall remain in effect, including, without limitation, any license rights, limitation of liability or indemnification provisions.

7.5. **Notice.** All notices or other communication required or permitted to be given under this

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

DPA must be in writing and given by e-mail transmission, sent to the designated representatives listed below:

The designated representative for the Provider for this DPA is:

Privacy Office

email: privacy@code.org

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

7.6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege. For clarity, nothing in this Section prohibits Provider from amending the Service Agreement pursuant to the amendment provisions set forth therein.

7.7. **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.

7.8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA SIGNING THE DPA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY THE LEA RESIDES IN, OF THE STATE OF THE LEA SIGNING THE DPA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7.9. **Waiver.** No delay or omission of the LEA or Provider to exercise any right hereunder shall be construed as a waiver of any such right and the LEA or Provider (as applicable) reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

7.10. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

7.11. **Electronic Signature:** The Parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with applicable state and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of their electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

7.12. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

[*Signatory Information Follows*]

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

CODE.ORG

By: DocuSigned by: Cameron Wilson ED2D85824BA6481...

Name: Cameron Wilson

Title: Chief Operating Officer

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

Date: 8/26/2020 | 14:41:11 PDT

LEA

By: DocuSigned by: Terry English C897B03169E74D2...

Authorized Representative: Terry English

School District: Falconer Central School District

Title: Data Privacy Officer

Address: Falconer Central Schools
2 East Ave, N
Falconer, NY 14733

Date: 10/15/2020 | 12:00:17 PDT

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

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

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

EXHIBIT "B"

SCHEDULE OF DATA

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

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	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program- student reads below grade level)	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

Parent/Guardian Contact Information	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
(Other)		
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify	

Student work	Student generated content; writing, pictures, projects, etc.	X

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

EXHIBIT "C"

DEFINITIONS

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

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

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

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

"**NIST Cybersecurity Framework**" shall mean the U.S. Department of Commerce National Institute of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 or any later standards developed by NIST.

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

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

"Program Communications" shall mean in-app or emailed communications relating to Provider's educational services, including prompts, messages and content relating to the use of the Service, for example; onboarding and orientation communications, prompts for students to complete, or teachers to assign exercises or provide feedback as part of the learning exercise, periodic activity reports, suggestions for additional learning activities in the Service, service updates (for example new features or content, including using for at-home learning opportunities), and information about special or additional programs (e.g. the Hour of Code) offered through the Services or Code.org website or application.

"Sell" consistent with the Future of Privacy Forum Student Privacy Pledge, does not include or apply to a purchase, merger or other type of acquisition of a company by another entity, provided that the company or successor entity continues to treat the Personally Identifiable Information contained in Student Data in a manner consistent with this DPA with respect to the previously acquired Personally Identifiable Information contained in Student Data. Sell also does not include sharing, transferring or disclosing Student Data with a Service Provider that is necessary to perform a business purpose (such as detecting security incidents, debugging and repairing, analytics, storage or other processing activities) provided that the Service Provider does not Sell the Student Data except as necessary to perform the business purpose. Provider is also not "selling" personal information if a user directs Provider to intentionally disclose Student Data or uses Code.org to intentionally interact with a third party, provided that such third party also does not Sell the Student Data.

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

"School Official" means for the purposes of this DPA and pursuant to FERPA (34 CFR 99.31

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

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

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

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

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

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF STUDENT DATA

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

1. Extent of Disposition

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

[Insert categories of data here]

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

2. Nature of Disposition

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

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

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

3. Timing of Disposition

Student Data shall be disposed of by the following date:

__ As soon as commercially practicable

4. Signature

_____
(Authorized Representative of LEA

_____
Date

5. Verification of Disposition of Data

_____
Authorized Representative of Company

_____
Date

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

EXHIBIT "E"

DATA SECURITY REQUIREMENTS

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

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

EXHIBIT "F"

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to Section 2-d of the New York State Education Law ("Education Law §2-d"), parents and eligible students are entitled to certain protections regarding confidential student information. school district name School District (the "District") is committed to safeguarding personally identifiable information from unauthorized access or disclosure as set forth below: Any terms not defined herein, shall have the meaning set forth in Education Law §2-d and if not defined in Education Law §2-d, in the Code.org Student Data Privacy Addendum (DPA) to which this document is an Exhibit.

1. A student's personally identifiable information cannot be Sold or released for any commercial purposes;

2. Parents have the right to inspect and review the complete contents of their child's education record maintained by the District;

3. State and federal laws protect the confidentiality of personally identifiable information. The District is committed to implementing safeguards associated with industry standards and best practices under state and federal laws protecting the confidentiality of personally identifiable information, including but not limited to, encryption, firewalls, and password protection when data is stored or transferred;

4. A complete list of all Student Data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or by writing to the NYS Education Department, Information & Reporting Services, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234;

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to the District;

6. The District has entered into contracts with certain third-party contractors/consultants who have received Student Data and/or teacher data and/or principal data. These contracts will include the following supplemental information:

   - The exclusive purpose(s) for which the Student Data will be used;
   - The commencement and termination dates of each such contract;
   - A description of how the Student Data will be disposed by the contractor upon expiration of the contract;
   - If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the Student Data or teacher or principal data that is collected; and
   - The data storage and security measures undertaken for Student Data or teacher or principal data, including whether such data will be encrypted.

7. Agreements with third party contractors/consultants will ensure that the subcontractors, persons or entities that the third party contractor will share the Student Data or teacher or principal data with, if any, will abide by data protection and security requirements.

Name of District: Falconer Central School District

Address: 2 East Ave, N
Falconer, NY 14733

District Authorized Representative full name: Terry English

Title: Data Privacy Officer

District Authorized Representative signature: DocuSigned by: Terry English C897B03169E74D2...

Date: 10/15/2020 | 12:00:17 PDT

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

Exhibit "G"
Supplemental Information

District and Code.org have entered into a Student Data Protection Addendum ("DPA"). The DPA supplements the Service Agreement and together with the Service Agreement, is collectively referred to as the "Agreement". The Service Agreement is defined as the Code.org Terms of Service located at https://code.org/tos (the "Service Agreement"). All terms not defined below or in the DPA shall have the meaning set forth in New York State Education Law §2-d ("Education Law §2-d").
required by Education Law §2-d(3)(c) and Section 121.3 of the implementing Regulations, the following is the "Supplemental Information" for the Agreement with the Contractor Code.org:

A. Use of Student Data: Student Data and/or Teacher or Principal Data which the Contractor comes into possession as part of its Agreement with the District shall be used for the following exclusive purpose(s):

Pursuant to and as fully described in the Service Agreement, Provider has agreed to provide the digital educational services set forth below and any other products and services that Provider may provide now or in the future (the "Services").

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

B. Service Providers: The Contractor will ensure that any and all subcontractors, or other authorized persons or entities that the Contractor may disclose the Student Data and/or Principal or Teacher Data with, if any, ("Service Providers") will abide by the applicable data protection and security terms of the DPA and in Education Law §2-d and Part 121 of the Regulations. Contractor will do so by entering into written agreements with such Service Providers, whereby the Service Providers agree to protect Student Data and/or Principal or Teacher Data (if applicable) in a manner no less stringent than the terms of the DPA. The list of Provider's current Service Providers can be accessed through the Provider's Privacy Policy (which may be updated from time to time).

C. Term and Termination:

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

- **Term:** The duration of this Agreement coincides with the duration of the parties' underlying Service Agreement, which is currently set to expire on**:** The Service Agreement expires upon termination by either party as set forth in the Service Agreement or upon a material breach by either Party of the terms of the DPA.

- **Data Deletion upon Termination:** When the Agreement between the District and the Contractor expires or terminates, the Contractor shall: At District's request, dispose of or delete all Personally Identifiable Information contained in Student Data within a reasonable time period following a written request. If no written request is received, Contractor shall dispose of or delete all Personally Identifiable Information contained in Student Data at the earliest of (a) when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law. Nothing in the DPA authorizes Contractor to maintain Personally Identifiable Information contained in Student Data obtained under the Agreement beyond the time period reasonably needed to complete the disposition, unless a student, parent or legal guardian of a student chooses to establish and maintain a separate Personal Login with Contractor to retain Student Generated Content. Disposition shall include (1) the shredding of any hard copies of any Personally Identifiable Information contained in Student Data; (2) erasing any Personally Identifiable Information contained in Student Data; or (3) otherwise modifying the Personally Identifiable Information contained in Student Data to make it unreadable or indecipherable or De-Identified or maintained to use with a Personal Login, pursuant to the other terms of the DPA. Contractor shall provide written notification to District when the Personally Identifiable Information contained in Student Data has been disposed pursuant to the District's request for deletion. The duty to dispose of Student Data shall not extend to data that has been De-Identified.

D. **Parent Access and Challenges to Accuracy of Student Data**: District shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information contained in the related student's Education Records and correct erroneous information, consistent with the functionality of Services. Contractor shall cooperate and respond within thirty (30) days to the District's request for Personally Identifiable Information contained in the related student's Education Records held by the Contractor to view or correct as necessary. In the event that a parent/legal guardian of a student or other individual contacts the Contractor to review any of the Education Records or Student Data accessed pursuant to the Services, the Contractor shall refer the parent or individual to the District who will follow the necessary and proper procedures regarding the requested information, provided however, that Contractor may also allow for direct access requests (but not correction or deletion rights) of Student Data and/or Education Records from a verified parent.

E. **Security and Storage**: The District and the Contractor hereby agree that the Student Data and/or Principal or Teacher Data (if applicable) shall be stored in the following manner: Contractor agrees to employ administrative, physical, and technical safeguards consistent with industry standards designed to protect Student Data and/or Teacher Data (if applicable) from unauthorized access, disclosure, use or acquisition by an unauthorized person, including when transmitting and storing such information. Contractor will not materially decrease the overall security of the Services during the term of the Agreement. The general security duties of Contractor are set forth below. Please see Contractor's Security Whitepaper for more details: https://code.org/about/InformationSecurityPolicy.pdf .

These measures shall include, but are not limited to:

- **Passwords and Employee Access**. Contractor shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3.

DocuSign Envelope ID: 72A97967-BE0F-4860-8E44-69CD7775F3FC

Contractor shall only provide access to Student Data to employees, contractors or Service Providers 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 Data shall pass criminal background checks in compliance with state and local ordinances.

- **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data, including ensuring that Student Data may only be viewed or accessed by parties legally allowed to do so. Contractor shall maintain all Student Data obtained or generated pursuant to the Agreement in a secure computer environment and not copy, reproduce, or transmit Student Data obtained pursuant to the Agreement except as necessary to fulfill the purpose of data requests by District or as otherwise set forth in the Agreement. The foregoing does not limit the ability of the Contractor to allow any necessary Service Providers to view or access data as set forth in the DPA.
- **Employee Training**. The Contractor shall provide periodic security training to those of its employees who operate or have access to the Services.
- **Security Technology**. When the Service is accessed using a supported web browser, the Provider will ensure that Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect Student Data from unauthorized access. The security measures employed shall include server authentication and data encryption at rest and in transit. Provider shall host Student Data pursuant to the Agreement in an environment using a firewall that is periodically updated according to industry standards.
- **Periodic Risk Assessment**. Contractor further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
- **Backups.** Contractor agrees to maintain backup copies of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.