DENVER PUBLIC SCHOOLS

DATA PROTECTION ADDENDUM

This Data Protection Addendum ("Addendum") is by and between School District No. 1 in the City and County of Denver and State of Colorado, d/b/a Denver Public Schools ("District") and Code.org ("Contractor"). This Addendum applies to all services provided by Contractor to District, whether by contract, service order, purchase order, invoice, or other form of agreement (the "Contract"). The Addendum and the Contract are collectively referred to hereinafter as "Agreement". This Addendum supersedes the Contract by adding to, deleting from and modifying the Contract as set forth herein. To the extent any such addition, deletion or modification results in any conflict or inconsistency between the Contract and this Addendum, this Addendum shall govern and the terms of the Contract that conflict with this Addendum or are inconsistent with this Addendum shall be of no force or effect.

In consideration of the mutual covenants, promises, understandings, releases and payments described in the Contract and this Addendum, the parties agree to amend the Contract by adding the following language:

1. Definitions

1.1. "*Act*" means the Colorado Student Data Transparency and Security Act, C.R.S. § 22-16-101 et seq., as amended from time to time.

1.2. "*Biometric Record*," as used in the definition of "Personally Identifiable Information," means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

1.3. "*Click-Wrap*" means both the act of accepting on-line terms and conditions of a Suppliers Agreement without ink or paper, by clicking on an on-line button or link for that purpose, and the resulting agreement.

1.4. "*Contract*" means the Code.org Terms of Service (code.org/tos) dated December 14, 2022 as updated from time to time, and any other form of agreement signed between the District and Contractor.

1.5. "*Designated Representative*" means District or Contractor employees as specified on Schedule 1 to whom all notices required in this Addendum will be sent.

1.6. "*District Data*" means any Personally Identifiable Information, Record, Education Records, as defined herein, and all Personally Identifiable Information included therein or derived therefrom that is not intentionally made generally available by the District on public websites or publications but is made available directly or indirectly by the District to Contractor or that is otherwise collected or generated by Contractor in connection with the performance of the Services, as defined herein.

1.7. "*De-identified Data*" means District Data from which all Personally Identifiable Information, as defined herein, and attributes about such data, have been permanently removed so that no individual identification can be made.

1.8. "*Education Records*" means records, files, documents and other materials that: (a) contain information directly related to a student; and (b) are maintained by the District, or by a party acting for the District such as Contractor.

1.9. "*End User*" means individuals authorized by the District to access and use the Services as defined herein.

1.10. "*Incident*" means a suspected, attempted, or imminent threat of unauthorized access, use, disclosure, breach, modification, disruption or destruction to or of District Data.

1.11. "*Mine*" means the act of searching through, analyzing, accessing, or extracting District Data, metadata, or information not necessary to accomplish the Services or purpose(s) of this Agreement for the benefit of the District.

1.12. "*Personally Identifiable Information*" or "*PII*" means information and metadata that, alone or in combination, is linked or linkable to a specific student so as to allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. Personally Identifiable Information includes, but is not limited to: (a) the student's name; (b) the name of the student's parent or other family members; (c) the address or phone number of the student or student's family; (d) personal identifiers such as the student's state-assigned student identifier, social security number, student number or biometric record; (e) indirect identifiers such as the student's date of birth, place of birth or mother's maiden name; and (f) demographic attributes, such as race, socioeconomic information, and gender.

To the extent it is not already included in the definition hereinabove, PII also includes: (a) "personal information" as defined in the Colorado Open Records Act, C.R.S. 24-72-101 et seq. ("CORA"); (b) Personally Identifiable Information contained in student "education records" as that term is defined in the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; (c) "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (d) "nonpublic personal information" as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (e) credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; and (f) other financial account numbers, access codes, and state- or federal-identification numbers such as driver's license, passport or visa numbers.

1.13. "*Record*" means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

1.14. "*Securely Destroy*" means to remove District Data from Contractor's systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in National Institute of Standards and Technology ("NIST") Special Publication 800-88 Guidelines for Media Sanitation (December 2014), or such other standard to which the District's Chief Privacy Officer or designee may agree in writing, so that District Data is permanently irretrievable in Contractor's and its Subcontractors' normal course of business.

1.15. "*Security Breach*" means an event in which District Data is exposed to unauthorized disclosure, access, alteration or use or a system configuration that results in a documented unsecured disclosure, access, alteration or use, in a manner not permitted in this Addendum, which poses a significant risk of financial, reputational or other harm to the affected End User or the District.

1.16. "*Services*" means what that term is defined in the Contract, and also includes any goods or services acquired by the District from the Contractor, including but not limited to computer software, mobile applications (apps), and web-based tools accessed by End Users through the Internet, installed or run on a computer or electronic device.

1.17. "*Subcontractor*" means Contractor's subcontractors, agents, or any other third party identified on <u>Schedule 2,</u> as updated by Contractor from time to time in accordance with the requirements of this Addendum, who Contractor has engaged to enable Contractor to perform its obligations under the Contract.

1.18. "*Student Profile*" means a collection of PII data elements relating to a student of the District.

1.19. "*Vendor Agreement*" means any form of agreement or documentation provided by the Contractor, including without limitation, an on-line agreement, proposal, or invoice, whether made a part of the Agreement or effective or purporting to be effective outside of the Agreement.

2. Rights and License in and to District Data

District owns all rights, title, and interest in and to District Data and any and all now known or hereafter existing intellectual property rights associated therewith, and any derivative works thereof or modifications thereto, including without limitation, De-identified Data. The District hereby grants to Contractor a limited, nonexclusive license to use District Data solely for the purpose of performing its obligations specified in the Contract. This Agreement does not give Contractor any rights, title, or interest implied or otherwise, to District Data or De-identified Data, except as expressly stated in the Contract.

3. Data Privacy

3.1. Use of District Data. Contractor shall use District Data only for the purpose of performing the Services and fulfilling its duties under the Contract.

3.2. Prohibited Uses of District Data. With the exception of De-identified Data that the District has agreed in writing to allow Contractor to use as specified in Section 3.5, Contractor shall not:

3.2.1. Use, sell, rent, transfer, distribute, alter, mine, or disclose District Data (including metadata) to any third party without the prior written consent of the District, except as required by law;

3.2.2. Use District Data for its own commercial benefit, including but not limited to, advertising or marketing of any kind directed toward children, parents, guardians, or District employees, unless such use is specifically authorized by this Agreement or otherwise authorized in writing by the District;

3.2.3. Use District Data in a manner that is inconsistent with Contractor's privacy policy;

3.2.4. Use District Data to create a Student Profile other than as authorized or required by the Contract to perform the Services; and

3.2.5. Store District Data outside the continental United States unless Contractor has given the District Designated Representative advance written notice of where and how the servers are housed, managed, and secured, and that the security standards required herein can be achieved.

3.3 Qualified FERPA Exception. If Contractor will have access to Education Records, Contractor acknowledges that, for the purposes of this Agreement, pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regulations, 34 C.F.R. Part 99 ("FERPA"), it will be designated as a "school official" with "legitimate educational interests" in the District Education Records and PII disclosed pursuant to the Contract, and Contractor agrees to abide by the FERPA limitations and requirements imposed on school officials. Contractor will use the Education Records only for the purpose of fulfilling its duties under the Contract for District's and its End Users' benefit, and shall not share District Data with or disclose it to any third party except as provided for in the Agreement, as required by law, or if authorized in writing by the District. Contractor warrants and represents that during the five-year period preceding the Effective Date of this Agreement, it has not been found in violation of FERPA by the U.S. Department of Education's Family Policy Compliance Office.

3.4 Subcontractor Use of District Data. To the extent necessary to perform its obligations specified in the Contract, Contractor may disclose District Data to Subcontractors pursuant to a written agreement, specifying the purpose of the disclosure and providing that: (a) Subcontractor shall not disclose District Data, in whole or in part, to any other party; (b) Subcontractor shall not use any District Data to advertise or market to students or their parents/guardians; (c) Subcontractor shall access, view, collect, generate and use District Data only to the extent necessary to assist Contractor in performing its obligations specified in the Contract; (d) at the conclusion of its/their work under its/their subcontract(s) Subcontractor shall, as directed by the District through Contractor, Securely Destroy all District Data in its/their possession, custody or control, or return such District Data to the District, at the election of the District; (e) Subcontractor shall indemnify the District in accordance with the terms set forth in Section 10 of this Addendum; and (f) Subcontractor shall utilize appropriate administrative, physical and technical safeguards in accordance with industry standards and best practices to secure District Data from unauthorized disclosure, access and use. Contractor shall ensure that its employees and Subcontractors who have potential access to District Data have undergone appropriate background screening, to the District's satisfaction, and possess all needed qualifications to comply with the terms of this Addendum. Contractor shall also ensure that its Subcontractors comply with the insurance requirements specified in Section 11 of this Addendum.

3.5 Use of De-identified Data. Contractor may use De-identified Data for purposes of research, the improvement of Contractor's products and services, and/or the development of new products and services. In no event shall Contractor or Subcontractors re-identify or attempt to re-identify any De-identified Data or use De-identified Data in combination with other data elements or De-identified Data in the possession of a third-party affiliate, thereby posing risks of re-identification.

3.6 Privacy Policy Changes. As required by § 22-16-108(2) of the Act, prior to making a material change to Contractor's privacy policies, Contractor shall send District's Designated Representative written notice, which includes a clear explanation of the proposed changes.

3.7 Misuse/Unauthorized Release. Upon discovering the misuse or unauthorized release of Personally Identifiable Information held in connection with this Agreement by Contractor, a Subcontractor or a subsequent Subcontractor of Contractor, Contractor will notify the District as soon as possible, regardless of whether the misuse or unauthorized release is a result of a material breach of the terms of this Agreement.

4. Data Security

4.1. Security Safeguards. Contractor shall maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of District Data. Contractor shall store and process District Data in accordance with industry standards and best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in CIS Critical Security Controls (CIS Controls), as amended, to secure such data from unauthorized access, disclosure, alteration, and use. Contractor shall ensure that all such safeguards, including the manner in which District Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with all applicable federal and state data protection and privacy laws, regulations and directives, including without limitation the Act, as well as the terms and conditions of this Addendum. Without limiting the foregoing, and unless expressly agreed to the contrary in writing, Contractor warrants that all electronic District Data will be encrypted in transmission and at rest in accordance with NIST Special Publication 800-57, as amended, or such other standard as the District's Chief Privacy Officer or designee may agree to in writing. Contractor shall also encrypt any backup, backup media, removable media, tape, or other copies. In addition, Contractor shall fully encrypt disks and storage for all laptops and mobile devices.

4.2. Risk Assessments. Contractor shall conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

4.3. Audit Trails. Contractor shall take reasonable measures, including audit trails, to protect District Data against deterioration or degradation of data quality and authenticity, and to ensure data is de-identified in accordance with this Addendum.

4.4. Reserved.

4.5. Background Checks.

4.5.1. If Contractor does not provide direct services to students, but has access to District Data, the Contractor and every person, including any subcontractor or agent of the Contractor, shall be required to have a criminal background check per Contractor's internal employment policies. "Direct services to students" includes, but is not limited to: instruction; physical, mental, and social health supports; transportation; and food services, which are provided to students at least one time per month during the school year.

4.5.2. If Contractor provides direct services to students and has access to student data, the Contractor and every person, including any subcontractor or agent of the Contractor, shall be required to have a criminal background check that meets the requirements of § 22-32-109.7, C.R.S. and other District requirements, including a fingerprint-based conviction investigation. Conducting a Colorado Bureau of Investigation criminal history check or a Name Check investigation for any person providing services under this Contract does not meet District requirements. The costs associated with the background checks are solely the Contractor's responsibility. Thereafter, any personnel, subcontractor, volunteer or agent hired or added during the term of this Contract shall satisfy the requirements set forth in this Section before performing services on Contractor's behalf. The Contractor shall make the background check results available upon request of the District in compliance with the provisions of § 24-72-305.3, C.R.S. The District also reserves the right to conduct its own criminal background check of every person before Services begin.

4.5.3. Notwithstanding the criminal background check requirement as set forth above, Contractor hereby certifies that no employee, subcontractor, volunteer or agent of the Contractor performing the Services has been convicted in Colorado or in any other State of a criminal offense involving: (i) the abuse, abduction, sexual molestation, physical or sexual assault on, or rape of a minor; or (ii) any crime involving exploitation of minors, including but not limited to, child pornography offenses or any crime of violence. Contractor shall notify the District immediately upon the discovery or receipt of any information that any person performing services on Contractor's behalf has been detained or arrested by a law enforcement agency of the aforementioned crimes. Contractor understands that allowing any employee, subcontractor, volunteer or agent of the Contractor performing the Services who has been arrested or convicted of the aforementioned crimes to: (i) provide direct services to students, (ii) access student data, or (iii) enter onto District property, constitutes a material breach of this Contract and may result in the immediate termination of this Contract and referral to law enforcement for possible criminal charges, or additional civil sanctions pursuant to federal and state law. Misdemeanor conviction(s) may not necessarily result in the immediate termination of this Contract. Misdemeanor convictions are evaluated on a case-by-case basis, considering the nature and gravity of the offense, time elapsed since the offense, conviction, or time served, and the nature of the Services. Upon the District's request, the Contractor shall provide documentation of every person performing the Services to substantiate the basis for this certification.

4.5.4. The Contractor and every person, including any subcontractor or agent of the Contractor, performing the Services, or who is on District's property, may be scanned through the Visitor Management System. If an individual's identity cannot be verified through an acceptable form of identification (driver's license or state ID), they will not be allowed on District's property.

5. Security Incident and Security Breach

5.1. Security Incident Evaluation. In the event of an Incident, Contractor shall follow industry best practices to fully investigate and resolve the Incident, and take steps to prevent developments that may result in the Incident becoming a Security Breach at Contractor's expense in accordance with applicable privacy laws.

5.2. Response. Immediately upon becoming aware of a Security Breach, or a complaint of a Security Breach, Contractor shall notify the District Designated Representative in writing as set forth herein, fully investigate the Security Breach, cooperate fully with the District's investigation of and response to the Security Breach, and use best efforts to prevent any further Security Breach at Contractor's expense in accordance with applicable privacy laws. Except as otherwise required by law, Contractor shall not provide notice of the Security Breach directly to individuals whose Personally Identifiable Information was involved, to regulatory agencies, or to other entities, without first providing written notice to the District's Designated Representative.

5.3. Security Breach Report. If the District reasonably determines that Contractor has committed a Security Breach, then the District may request Contractor to submit, within seven (7) calendar days from discovery of such breach, a written report, and any supporting documentation, identifying (i) the nature of the Security Breach, (ii) the steps Contractor has executed to investigate the Security Breach, (iii) what District Data or PII was used or disclosed, (iv) who or what was the cause of the Security Breach, (v) what Contractor has done or shall do to remediate any deleterious effect of the Security Breach, and (vi) what corrective action Contractor has taken or shall take to prevent a future Incident or Security Breach. The District reserves the right to require the Contractor to amend its remediation plans.

5.4. Effect of Security Breach. Upon the occurrence of a Security Breach, the District may terminate this Agreement in accordance with District policies. The District may require Contractor to suspend all Services, pending the investigation and successful resolution of any Security Breach, and Contractor may be required to reimburse District all amounts paid for any period during which Services were not rendered. Contractor acknowledges that, as a result of a Security Breach, the District may also elect to disqualify Contractor and any of its Subcontractors from future contracts with the District.

5.5. Liability for Security Breach. In addition to any other remedies available to the District under law, contract, or equity, Contractor shall reimburse the District in full for all costs, including but not limited to, payment of reasonable legal fees, reasonable audit costs, fines, and other fees imposed that were actually incurred by the District and to the extent such costs are attributable as a result of any act or omission by Contractor or Contractors Subcontractors for any Security Breach. If required by law or contract, Contractor shall provide notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities.

6. Response to Legal Orders, Demands or Requests for Data

6.1. Received by Contractor. Except as otherwise expressly prohibited by law, Contractor shall immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Contractor seeking District Data; consult with the District regarding its response; cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and, upon the District's request, provide the District with a copy of its response.

6.2. Received by District. If the District receives a subpoena, warrant, or other legal order, demand or request seeking District Data maintained by Contractor, including but not limited to, a request pursuant to the CORA, the District will promptly notify Contractor and, within two (2) business days, excluding national holidays, Contractor shall supply the District with copies of the District Data for the District to respond.

6.3. Parent Request. If a parent, legal guardian or student contacts the District with a request to review or correct District Data or PII, pursuant to FERPA or the Act, the District will promptly notify Contractor's Designated Representative and Contractor shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District, within ten calendar (10) days after receipt of District's notice. Conversely, if a parent, legal guardian or student contacts the Contractor with a request to review or correct District Data or PII, within ten calendar (10) days after receipt of such notice, Contractor shall promptly notify the District and shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District.

6.4. Access to District Data. District shall have the right to access and retrieve any or all District Data stored by or in possession of Contractor upon written notice to Contractor's Designated Representative. Contractor shall make the District Data available to the District within seven (7) calendar days from the date of request.

7. Compliance with Applicable Law

7.1. School Service Contract Providers. If Contractor provides a "school service", which is defined as an Internet website, online service, online application or mobile application that: (a) is designed and marketed primarily for use in a preschool, elementary school or secondary school; (b) is used at the direction of District teachers or other District employees; and (c) collects, maintains or uses District Data or PII, then Contractor is a "school service contract provider" under the Act. If that is the case, Contractor must complete Schedule 5. Contractor shall update Schedule 5 as necessary to maintain accuracy. District reserves the right to terminate the Contract, or the DPA, or both, as specified in Section 8, should the District receive information after the Effective Date that significantly modifies Contractor's representations made in this Section 7.1.

7.2. Children's Online Privacy and Protection Act. If Contractor collects personal information (as defined in the Children's Online Privacy and Protection Act of 1998, 5 U.S.C. 6501 to 6505, and its implementing regulations ("COPPA")) from children under thirteen (13) years of age in performing the Services, Contractor warrants, represents, and covenants that such collection is and shall be for the use and benefit of the District and for no other commercial purpose. Contractor has provided the District with written notice of its collection, use, and disclosure practices.

7.3. Compliance with Laws. Contractor warrants that it will abide by all applicable laws, ordinances, rules, regulations, and orders of all governmental agencies or authorities having jurisdiction over the Services including but not limited to: (a) COPPA; (b) FERPA; (c) the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (d) the Health Information Technology for Economic and Clinical Health Act, (e) Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (f) Payment Card Industry Data Security Standards; (g) Protection of Pupil Rights Amendment, 20 U.S.C. 1232h, 34 C.F.R. Part 98; and (h) Americans with Disabilities Act, and Federal Export Administration Regulations.

7.4. Americans with Disabilities Act. To the extent the District is required to provide accommodations in compliance with the Americans with Disability Act ("ADA"), Contractor will require that its system and services will, at a minimum, conform with all laws, regulations and guidance that apply to accessibility in accordance with the ADA, Section 504 of the Rehabilitation Act of 1973; provided, however, Contractor will have no obligations with respect to such compliance as it relates to any portion of the system and services provided or developed by the District including District content.

8. Term and Termination

8.1. This Addendum takes effect immediately as of the Effective Date, and remains in full force and effect until the successful completion of the services, unless earlier terminated under Sections 8.3 or 12.3.

8.2. Subject to Sections 8.3 and 12.3, this Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Contract between the Parties or successful completion of the Services. Alternatively, upon re-execution of the Contract by the authorized persons of District and Contractor, this Addendum shall also be revived and be of full force and effect.

8.3. Termination by the District.

8.3.1. The District may immediately terminate the Contract in accordance with District policies if, at any time, the District determines in its sole discretion, that Contractor has breached any of the requirements of this Addendum.

8.3.2. The District may terminate the Contract if the District receives information that Contractor has failed to comply with the same or substantially similar security obligations as set forth herein with another school district.

8.3.3. The District may terminate the Contract if the District receives information after execution of this Addendum, that any of Contractor's representations or warranties have substantially changed after execution of this Addendum, including but not limited to the terms of Contractor's privacy policy.

9. Data Transfer Upon Termination or Expiration

9.1. Destruction of District Data. With the exception of De-identified Data as set forth in Schedule 3 that District has specifically agreed in writing to allow Contractor to use after termination or expiration of this Agreement, or District Data for which Contractor has specifically obtained consent from the parent, legal guardian or student to keep, no later than thirty (30) calendar days after receipt of a written request from the District, and subject to the process outlined in Section 9.2, Contractor shall certify in writing that all District Data and PII that Contractor collected, generated or inferred pursuant to the Contract ("Contract Data"), is Securely Destroyed, pursuant to Schedule 4 attached hereto.

9.2. Destruction of District Data. The Services are intended for use both within schools (i.e., as part of classroom sections established by teachers in the K-12 setting) and outside of school (i.e., for use at home and not for K-12 school purposes). The same Code.org student account may be used by a student over time both in school and outside of school – which allows the student to retain and expand upon prior projects, review prior CS learnings, etc. If a student or parent creates a Code.org account using a personal login (i.e., using an email address and password – as opposed to a teacher-created account using a teacher-controlled picture password or secret word or an account created through the Clever rostering service) and enrolls the account in a teacher's section, or later adds a personal login to a teacher-created account or one created through a specific rostering service, the student will maintain certain control and access rights over the account even if it was originally established for a K-12 purpose.

For example, although a teacher can generally delete their own account and any student accounts enrolled solely in the teacher's section at any time, if a student enrolled in the teacher's section has created a personal login for their Code.org account, the student's Code.org account (and the student generated content associated with the account) will not be deleted at the sole request of the teacher or LEA - both the student and LEA/teacher would need to request deletion. Conversely, as long as the student remains part of a teacher's section, the student cannot unilaterally delete the account without asking the teacher to first remove them from the teacher's section. This ensures that the student retains access to their student-generated content and that the LEA retains access to any Educational Records in the account that the student might intentionally or inadvertently delete. Subject to the foregoing, a teacher, or student may delete their account at any time.

Notwithstanding the foregoing, if the District wishes to ensure the deletion of all Code.org student accounts enrolled in a District teacher's section (i.e., including those student accounts using a personal login), Code.org will do so based on the District's specific request made to privacy@code.org. This process requires that the District either (1) identify each teacher account with sections the District seeks to delete so that Code.org can identify student accounts enrolled in those teacher's sections (because Code.org does not maintain readable email addresses for student accounts - only a one-way hash of the email address – Code.org cannot directly identify student accounts even if the District email address domain was used to establish the personal login) or (2) request that Code.org identify all teacher accounts using a specific District email domain (e.g., xxx@LEA.org) and then work with Code.org to identify for deletion all or select sections under the identified teacher accounts. Code.org will then delete or de-identify all student accounts in those sections. The District is responsible for notifying students not to use student accounts they've previously created to enroll in teacher sections if the student may wish to ensure their student generated content can be retained despite a subsequent deletion request from the District.

In the absence of a deletion request by the teacher, or student (or the District with proper authentication showing control over the teacher/student accounts), the Code.org Personal Data Retention and Deletion Policy provides for automatic deletion or de-identification of Code.org student accounts after five (5) years of inactivity.

9.3. Response to Specific Data Destruction or Return Requests. After receiving a written request from the District, Contractor shall Securely Destroy or return any specific District Data or Contract Data that is in its possession or in the possession of its Subcontractors pursuant to the process outlined in Section 9.2, no later than thirty (30) calendar days after receiving a written request from the District.

10. Indemnification

10.1. If the Contractor is a "public entity" then it will be responsible for the negligent acts and omissions of its officers, agents, employees and representatives with respect to its obligations under this Agreement. Any provision of this Agreement, whether or not incorporated herein by reference, shall be controlled, limited and otherwise modified so as to limit any liability of the Contractor under the Colorado Governmental Immunity Act, C.R.S. 24-10-101 et seq. It is specifically understood and agreed that nothing contained in this paragraph or elsewhere in this Agreement shall be construed as an express or implied waiver of its governmental immunity or as an express or implied acceptance of liabilities arising as a result of actions which lie in tort or could lie in tort in excess of the liabilities allowable under the Act, as a pledge of the full faith and credit of the Partner, or as the assumption by the Partner of a debt, contract or liability of the District or its affiliates in violation of Article Xl, Section 1 of the Constitution of the State of Colorado.

10.2. If Contractor is not a "public entity" then Contractor shall indemnify, defend and hold District and its elected officials, employees, representatives, and agents harmless, without limitation, from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses, including attorneys' fees, the costs of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from Contractor's, or Contractors subcontractors, performance of services under this Addendum, any third-party claim against any Indemnified party to the extent arising out of or resulting from Contractor's, or Contractors subcontractors, failure to comply with any of its obligations under Sections 3, 4, 5, and 9 of this Addendum, and any breach of Contractor's, or Contractors subcontractors, obligations under this Addendum. These indemnification duties shall survive termination or expiration of this Agreement.

11. Insurance

11.1 Coverage. As required by Schedule 6.

12. EULAs, Terms of Use, and other License Agreements

12.1. The Contractor grants such licenses and user permissions and provides the Services under those conditions as set forth in Schedule 7 attached hereto.

12.2. Click-Wrap and Exclusions. If Schedule 7 is blank or not attached, the Contractor grants such licenses and user permissions as the District may accept by Click-Wrap, whether with the Contractor or provided through a Subcontractor. Notwithstanding any such Click-Wrap terms and conditions, and notwithstanding the provisions in the Agreement or Vendor Agreement, the District DOES NOT agree to any of the following:

12.2.1. Jurisdiction, venue and governing law other than Colorado.
12.2.2. Indemnification by the District of any person.
12.2.3. Binding arbitration or any other binding extra-judicial dispute resolution process.
12.2.4. Limitation of Contractor's liability for (i) direct damages; (ii) bodily injury, death or damage to tangible property or (iii) amounts that are less than the insurance coverage the Contractor provides.
12.2.5. Ownership or use of District Data other than as described in this Addendum.
12.2.6. Confidentiality provisions in conflict with the District's obligations under the Colorado Open Records Act and other applicable open records laws.
12.2.7. Fees, penalties, and payment obligations other than as agreed to in the Agreement.

12.3. End Users. In the event that the Contractor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with End Users or with the District ("EULAs"), the Parties agree that the terms of this Addendum shall supercede the EULAs.

12.4. Subcontractor Click-Wrap. If the Contractor is providing software or on-line services through Subcontractors, and Click-Wrap will be required for the District to avail itself of the Services under this Agreement, then the Contractor shall cause the Subcontractor providing such software or on-line access to consent to and honor the terms of this Addendum with respect to the District's use of the Services provided through the Subcontractor.

13. Miscellaneous

13.1. Public Inspection of Agreement. Contractor acknowledges and agrees that this Agreement and all documents Contractor provides District as required herein, are public records for purposes of the CORA and shall at all times be subject to public inspection. The parties understand that in the event of a request for disclosure of such information, the District will notify Contractor to give Contractor the opportunity to redact its proprietary or confidential material. In the event of the filing of a lawsuit to compel disclosure, the District will tender Contractor's material to the court for judicial determination of the issue of disclosure and Contractor agrees to intervene in such lawsuit to protect and assert its claims of privilege against disclosure or waive the same.

13.2. Survival. The Contractor's obligations under Sections 3, 4, 5, 6, 9, and 10, and any other obligations or restrictions that expressly or by their nature are to continue after termination, shall survive termination of this Agreement for any reason until all District Data has been returned or Securely Destroyed.

13.3. Choice of Law. Any claim, controversy or dispute arising under or related to this Addendum shall be construed pursuant to the substantive, not conflicts, laws of the State of Colorado. Each of the Parties submits to the exclusive jurisdiction of any state court sitting in or federal court with jurisdiction over Denver County, Colorado, in any action or proceeding arising out of or relating to this Agreement and agrees that all claims in respect of the action or proceeding may be heard and determined in any such court. Each Party also agrees not to bring any action or proceeding arising out of or relating to this Addendum in any other court. Each of the Parties waives any defense of inconvenient forum to the maintenance of any action or proceeding so brought and waives any bond, surety or other security that might be required of any other Party with respect to any such action or proceeding.

13.4. Immunities. The District retains all of its rights, privileges and immunities under the Colorado Governmental Immunity Act, C.R.S. § 24-10-101 *et seq*.

13.5. No Assignment. Contractor shall not assign or subcontract any of its rights or obligations hereunder without the express written consent of the District. Any assignment in violation of this section shall be void.

13.6. No Third Party Beneficiaries. Nothing in this Agreement shall be construed to give any rights or benefits to anyone other than District.

13.7. Schedules. The following schedules are attached hereto, or shall be attached hereto, and are specifically made a part hereof by this reference:

Schedule 1 – Designated Representatives
Schedule 2 – Subcontractors
Schedule 3 – Written Consent to Maintain De-identified Data
Schedule 4 – Certification of Destruction\Return of District Data
Schedule 5 – Data Elements
Schedule 6 – Insurance
Schedule 7 – EULAs and Terms of Use

13.8. Counterparts. This Addendum may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

13.9. Electronic Signatures and Electronic Records. Each party consents to the use of electronic signatures by the other party. This Addendum, and any other documents requiring a signature under this Addendum, may be signed electronically by each party in the manner specified by the District. The parties agree not to deny the legal effect or enforceability of this Addendum solely because it is in electronic form or because an electronic record was used in its formation. The parties agree not to object to the admissibility of the Addendum in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party is signing this agreement on the date stated opposite that party's signature.

SCHOOL DISTRICT NO. 1 IN THE CITY AND COUNTY OF DENVER AND STATE OF COLORADO, D/B/A DENVER PUBLIC SCHOOLS

Date: Sep 6, 2023

By: ______________________

Staci Crum
Director, Financial Operations

CODE.ORG

Date: 9/6/2023 | 08:56:34 PDT

By: DocuSigned by:
Cameron Wilson
ED2D85824BA6481...

Cameron Wilson
President

SCHEDULE 1

Designated Representatives

DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Name: Jennifer Collins Title: Chief Privacy Officer, Deputy General Counsel Address: 1860 Lincoln St Denver, CO 80203 Phone: 720-423-2211 E-mail: legal_contracts@dpsk12.org	Name: Cameron Wilson Title: President Address: 801 Fifth Ave, Suite 2100 Seattle, WA 98104 Phone: (206) 420-1376 E-mail: Cameron@code.org and privacy@code.org

SCHEDULE 2

Subcontractors

Contractor shall update this information as necessary to maintain accuracy and shall send revised attachments, exhibits or schedules to the District's Authorized Representative.

What third party vendors does Contractor do business with that may have access to student personally identifiable data, and what is the purpose of these third party vendors (please complete the table below with this information)?

Name of Subcontractor	**Primary Contact Person**	**Subcontractor's Address**	**Subcontractor's Phone/email**	**Purpose of re-disclosure to Subcontractor**

Contractor does not "sub-contract" any portion of the Services to any entity acting as a "subcontractor" to perform its obligations under the Contract. However, like all modern organizations, Code.org does utilize third-party vendors to perform various services on behalf of Code.org, subject to contractual terms that prohibit the vendors' use of any personal data (including personally identifiable data) they may process on behalf of Code.org for any purposes other than providing the contracted service to Code.org. In some instances, student personally identifiable data (defined as "Student Data") may potentially be processed by such vendors on behalf of Code.org. Code.org maintains a current list of such vendors and the purpose of their processing, which is linked from the Code.org privacy policy. The current list can be found at the following link:

https://docs.google.com/spreadsheets/d/e/2PACX-1vQ_AYYT_4K9Hpc5LrL4QAeXUmEMQR7rAXrHtloM4yt3xNndqPh-ABHXy0SJHZQ8ZSDSFQQv7ZWdXQjj/pubhtml?gid=222345124&single=true

SCHEDULE 3

Written Consent to Maintain De-identified Data

The District hereby gives its consent for Contractor to retain and use for the stated purpose and period, De-identified Data elements as set forth below:

Description of De-identified Data Elements	Purpose for Retention and Use	Period of Use
Age	To analyze and improve the platform and curriculum, and measure our nonprofit impact	Indefinite
Grade Level	To analyze and improve the platform and curriculum, and measure our nonprofit impact	Indefinite
Race	To analyze and improve the platform and curriculum, and measure our nonprofit impact	Indefinite
Gender	To analyze and improve the platform and curriculum, and measure our nonprofit impact	Indefinite
Meta Data re: interaction with the application (e.g., progress data; grade level) disassociated from any potential personal identifier	To analyze and improve the platform and curriculum, and measure our nonprofit impact	Indefinite

I\We, Cameron Wilson, as President and the authorized representative(s) of the Contractor do hereby certify that no attempt will be made to re-identify De-identified Data.

Contractor Name: Code.org
Contractor Representative Name: Cameron Wilson
Title: President

DocuSigned by:
Cameron Wilson
ED2D85824BA6481...

Signature: ______________________ Date: 9/6/2023 | 08:56:34 PDT

SCHEDULE 4

Certification of Destruction\Return of District Data

I\We, ______[NAME(S)]____________________, as the authorized representative(s) of the Contractor do hereby acknowledge and certify under penalty of perjury that [initial next to both subparts of the applicable Part A or Part B]:

Part A - Destruction:

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was destroyed on __________________, 20___ by means of [describe destruction methods]: ____________________________________.

______ the District Data and PII provided to Contractors Subcontractors as part of the Data Protection Addendum in accordance with federal and state law was destroyed as set forth below:

Name of Subcontractor	*Date of Deletion*	*Destruction Method*

Part B - Return: [If this option is elected by the District, then Contractor shall also complete Part A.]

______ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District, on __________________, 20___ to ______________________________, by means of [describe destruction methods]: ____.

______ the District Data and PII provided to Contractors Subcontractors as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District as set forth below:

Name of Subcontractor	*Date of Return*	*Return / Transfer Method*

Contractor Name: ____

Contractor Representative Name: ____

Title: ____

Signature: ____ Date: ______________________

SCHEDULE 5

Data Elements

(Mandatory to be completed if the Contractor is a School Service Contract Provider under CRS 22-16-101 et seq.)

1. Contractor collects, generates or uses pursuant to the Agreement the following data elements of District Data or PII:

The following table describes the data that Code.org collects and stores if a User creates a Code.org Student or Teacher account for use with Code.org courses.

Data stored by Code.org if a User creates a Code.org Student account	How and when is the data collected?	How this data is used
Display Name (e.g., "Cool Coder" or "John") and username (e.g., "coolcoder7")	Required by User (or their Teacher) on account creation	Display name is used to provide Students a welcoming login and to identify the Student in the Teacher's roster view of student progress. Usernames are generated based on the initial display name and can be used along with a password to sign into an account.
Account passwords	Required by User (or their Teacher) on account creation.	Passwords are established by the User and can be updated through the User's account settings or by a Teacher that manages a section in which the Student is enrolled. They are used for User authentication at sign-in.

Secret words/pictures	System generated by Teacher when adding Student to section (if choosing not to use Student accounts with passwords).	Secret words or pictures are system generated, but can be reset by the Teacher. They are used for User authentication at sign-in.
Age (Not birthdate)	Required by User (or their Teacher) on account creation or first sign in before using the site.	This data is used to understand the developmental stage of Students in order to offer an age-appropriate experience for each Student. We also use this field to ensure we don't allow Students under age 13 to access age-restricted features (such as sharing their coding projects on social media). We store ages (e.g., 16), as opposed to birth dates (e.g., Feb 13, 2001).

One-way hash of student email address (NOT the actual email address, which is collected in the web browser but never transmitted to Code.org and thus never stored by us)	Email address is required (but not stored) on account creation if a Student creates an account, a Teacher creates the account via a third-party rostering provider, or the Student later adds a personal login to a Teacher-created account. Email address is not required if an account is created by a Teacher using a picture or secret word login for the section, though it can be optionally added by the Student later.	Where a Student creates a personal login (i.e., the student creates a Code.org account using an email address and selecting their own password - or adds a personal login to an existing account created by the Teacher on behalf of the Student through rostering or using picture or secret word logins), the Student's email address is only used for the purposes of login (along with the User's password). It is NOT stored by Code.org in a retrievable format. To protect Student privacy, we only store a one-way hash of the email address. We do not have any way of sending email to Students or retrieving their actual email addresses from their account. See Student Email Addresses below for more details.

Parent or guardian email address	Can be optionally provided by a parent to receive updates or create a login for their child at home. In some jurisdictions, we may require a Student under 13 to provide a parent or guardian email address for the purpose of obtaining consent to the creation of the Code.org account by the student.	Parents or guardians can choose to link their email address to their Student's account to receive updates from Code.org. (A student can also add the parent or guardian email address.) In some jurisdictions, we may require a parent or guardian email address for the purpose of consenting to the creation of a Student Code.org account for a Student under the age of 13. In those instances, the email address is used solely for that purpose and is linked to the Student account for purposes of allowing the parent to stay updated on their Child's progress and projects - and the Parent email address can also be used for password recovery and to request support.
Account Identifiers	System generated (separate identifiers may be provided by authentication services). This is NOT a student number assigned by a school.	These identifiers are used to maintain and operationalize accounts.

Login time, IP address, and other technical data	Automatically collected as the Services are used.	This data helps Code.org troubleshoot any problems Users experience. It also helps Code.org understand usage patterns, ensure the service can support all Users, and enable Services updates with minimal service disruption. See Technical Information below for more details.
Gender	Optionally provided by the Student or their Teacher.	This information is only used in aggregate to measure gender distribution and how Students respond to different computer science challenges, or track our aggregate progress towards reducing the gender gap in computer science.
Race	Optionally provided by the Student (only requested from Students 13 and over and only if their IP address is in the US).	Students aged 13 and over have an option to indicate their race. For Students under age 13 we do not ask individual race, but we ask the Teacher to optionally estimate the racial distribution of the entire classroom. This information is only used in aggregate, to measure the percentage of students from underrepresented racial and ethnic groups and their aggregate response to computer science challenges, and in order to track our aggregate progress toward improving diversity in computer science.

Progress in the course 1- Date/Time each lesson is tried 2- Number of tries to solve a level, and whether it was solved successfully or optimally 3- Information on how the Student solved the level including time to completion and whether they used hints 4- The code that the Student submitted 5- Student-provided answers to simple assessments (e.g., multiple-choice questions)	Collected as a Student works through a tutorial or course progression.	This information is displayed to Students and their Teachers to see their progress in a course, to see the code they've created, and to identify topics they need help with. It also lets Students pick up where they left off if they sign out and sign in later. See Technical Information below for more details. This data, in de-identified or aggregate form, also helps Code.org improve course effectiveness. For example, if a level is too hard, Code.org may take action (like providing better hints) to improve the learning process.

Student projects - apps, animations, stories, or code-art	Collected as a Student creates such projects. Creating apps and projects is part of our course progressions but can also be done outside our courses through our standalone tools.	The code and any associated data for these apps are stored by Code.org so Students can retrieve their projects each time they log in. When Students work in the context of a classroom, their Teacher also has access to view the projects created by any Students in the classroom. Student projects and code creations each have a custom URL that Students can use to share with others, or post to the Code.org public gallery. On the public gallery, projects are displayed with only the first letter of the Student's display name to protect Student privacy as well as their age. We do not allow Students under the age of 13 to share projects (e.g., in App Lab) to the Code.org public gallery when these projects allow for Student-uploaded content. Students may "remix" (copy and then change or improve upon) projects made by themselves or by other Users. Students age 13 or over can also, at their discretion, post their projects to their social media accounts. In our elementary school courses, Students create stories, games, or art using tools, such as Play Lab and Sprite Lab, which are generally limited to using artwork and sounds provided by Code.org or uploaded by their teacher. Where we do allow custom uploads by Students in these tools (e.g., uploading an image for a Student-created storyboard), Students are advised never to upload any media containing Personal Information and we implement controls that block Student sharing of projects to the Code.org public gallery that contain

		custom uploads. Students can write dialogues for these projects. Some text provided by Students in these tools is automatically analyzed and moderated to help prevent sharing of personal data like email addresses and phone numbers. Our middle school and high school courses teach Students to make more complex apps and games, such as App Lab, Game Lab, and Web Lab. These tools allow the Students to upload custom photos, sounds and/or videos. (See below)

Student-uploaded images, sounds, or videos	Collected if a Student chooses to upload custom files.	Only Students age 13 and older, or Students under 13 who are working in a classroom whose Teacher has added the Student to a class section, can choose to upload custom images, sounds, and videos to the Code.org platform to use within apps or games that they create in programing tools as part of our courses for grades 6+ (App Lab, Game Lab, and Web Lab). Students under 13 are advised never to upload any media containing Personal Information and we do not allow Students under the age of 13 to share projects created using these tools to the Code.org public gallery. Similarly, where custom uploads are allowed for programming tools intended for younger students (e.g, Play Lab and Sprite Lab), Students are advised never to upload any media containing Personal Information and we implement controls that block Student sharing of projects that contain custom uploads. These files are not used by Code.org for any purpose other than within these projects. These projects may be shared and remixed as described above, subject to those restrictions described.

Data collected by Student-created apps	Collected if users of a code project created by the Student choose to enter data into the app.	Students may use Code.org to create their own apps. Depending on the app author's design, a Student-created app may in turn collect data by prompting other Users (anybody who tries using the Student-created app) to enter information, such as a favorite movie. If a Student creates an app that collects and stores data in this fashion, all data entered by Users of the app may be accessed and possibly shared publicly by the app author, the app itself, and potentially anybody with a link to view the app. Code.org does not itself use or share this data outside of the app. Before using a Student-created app that collects data, Users are shown a clear warning that any data they enter may be shared publicly and that they should not share anything personal to them or to others.
Written comments in response to curricular/educational prompts within Code.org courses	Collected if a Student chooses to enter text in response to the prompts.	Within some of our courses, Students in a classroom are prompted to answer a question. Their answers are shared with any Teacher with whom the Student is affiliated on Code.org and are used by Code.org in de-identified form to improve the curriculum.

Student-provided responses to surveys (e.g., multiple choice and free response questions)	Collected if a Student chooses to fill out a survey offered inside the courses.	We may ask for responses to attitudinal questions (to assist the Teacher in understanding their classroom's reaction to learning computer science and, in de-identified or aggregate form, to help Code.org improve our curriculum). Students are informed that answers to these attitudinal questions are shared with the Teacher anonymously without their name attached. We may, however, share a Student's identity, answer, and other information related to a given question with their teacher or appropriate authorities if we are prompted to do so, and upon investigation, we have a good-faith and reasonable belief that the answer indicates the Student may harm themselves or others, among a few other limited scenarios outlined in the section titled "How We Share or Transfer Information." However, we are not actively monitoring student answers for such issues. If you are a teacher, please contact support@code.org so we can help you if your Student indicates they may be unsafe.

Additional* data stored by Code.org if a User creates a Code.org Teacher account	How and when is the data collected?	How this data is used

Email address	Email address is required at account creation (or when switching from a Student account to a Teacher account).	Email addresses are used to send emails to the Teacher with updates about their classroom or Student progress, send notices when new course-work is available, and provide updates on curriculum, tools, professional learning opportunities, etc. Teachers can choose at account creation whether to receive non-transactional emails (e,g., updates to our courses, local opportunities, or other computer science news). All non-transactional emails sent by Code.org contain an unsubscribe link and do not require typing a password to unsubscribe.
District and school name and/or school type (private, public, charter, homeschool, after school, organization, or other) and/or school address	Optionally provided by the Teacher at account creation or after creating an account.	At the Teacher's discretion and under their control, we will list their school in the Code.org map and database of schools that teach computer science courses. Code.org or our professional development partners may also use this information to reach out to the Teacher's school or district to discuss broader education partnerships or participation in special events.

Verified Teacher Identification Information	Optionally provided by the Teacher when seeking “verified teacher” status if the Teacher’s status cannot be demonstrated through other proof - such as verification of the teacher’s position on a school website.	At the Teacher's discretion, and under their control, they may provide a copy of an identification (such as a school-issued ID or a state-issued ID) to our support desk as part of demonstrating their teacher status. We recommend redacting data beyond name, photo, and issuing authority. All such images are deleted after the verification is complete.
Student section data	Collected if a Teacher decides to create a section on Code.org to manage their Students.	The Teacher may create accounts for their students (and provide each Student’s display name which the Teacher can manage using full names or initials, and, optionally, their age and gender) or direct students to create accounts themselves, and organize these Students into sections. The Teacher may assign each section a display name, a course assignment, and grade level. The section grouping data is used to simplify their view of Students across multiple sections. Teachers are encouraged to share a Code.org document with Students and parents informing them about enrollment in a Code.org section, including the privacy implications.

Survey and demographic data	Collected if a Teacher chooses to optionally fill out a survey.	For the purposes of evaluating our own work and improving our education results, Code.org regularly sends surveys to Teachers. These surveys are completely optional. The data provided by Teachers in these surveys is saved and used for analysis by Code.org, research partners, our Regional Partners, our International Partners, or facilitators. Any survey data shared with external parties is de-identified and aggregated.
Attendance at professional learning workshops	Collected when a Teacher attends a workshop.	Attendance of Teachers at our professional learning workshops is stored and associated with the Teacher's account on Code.org. This data may be shared (along with the Teacher's identity) with any other parties involved in the Teacher's professional learning, such as the facilitator who led the workshop, the professional learning organization hosting the workshop, or the school district of the Teacher. In some cases, the school district may use workshop attendance data to compensate Teachers for participating in the Code.org professional learning program.

Progress, answers, documents, projects, and peer reviews for online professional learning.	Collected as a teacher interacts with our online professional learning tools. Participation in professional learning programs is optional.	Progress and answers in online professional-learning courses for Teachers are stored in their Teacher account in order to allow Teachers to pick up where they left off. This includes the lesson plans, documents, and other projects Teachers create as part of finishing the online learning courses. After submitting a document or project, Teachers receive peer feedback from each other which is also stored so that they can read it. Teachers also take a self-assessment survey to create a custom learning plan. The results of this survey are stored with the Teacher's account along with their custom plan.
Comment feedback provided to students	Collected if a Teacher decides to give written comments to their Students on their work	The Teacher may provide written feedback to their Students on their coursework. Though a Student will only see the most recently provided comment on a given level, we store all the previously shared comments as part of the Teacher's account in case the Teacher or school needs to access them later.

* A Teacher account on Code.org has all the functionality of a Student account, and as a result the data collected and stored for a Teacher account is a superset of the data stored for a Student account.

2. Contractor collects and uses the District Data for the following educational purposes:

   See the Table above.

3. Contractor's policies regarding retention and disposal of District Data are as follows:

   Unless we receive a deletion request, we may retain data as long as a User account is active, as long as the personal data is necessary or useful for operational purposes, or as required under any contract or by applicable law. In the absence of a deletion request, the Code.org Personal Data Retention and Deletion Policy provides for automatic deletion or de-identification of Code.org student accounts after five (5) years of inactivity. We may indefinitely retain information which has been de-identified or aggregated such that it is no longer personal data.

4. Contractor uses, shares or discloses the District Data in the following manner:

   We use data to provide the Service, as set forth in the Table above. We do not rent or sell data or exploit it for financial gain in any other way. The limited circumstances in which we may share personal data (e.g., third-party service providers; student data shared with teachers, etc.) are set forth in our privacy policy at code.org/privacy.

5. Has Contractor's agreement has ever been terminated by another school district for failure to comply with the same or substantially similar security obligations as those set forth in this Agreement?

   □Yes X No.

   If yes, describe: N/A

SCHEDULE 6

Insurance

N/A

SCHEDULE 7

EULAs and Terms of Use

As part of its nonprofit mission to expand access to computer science, Code.org provides an online curriculum for teaching computer science, and an online learning platform for students to learn coding and computer science subject to the Code.org Terms of Services (at https://code.org/tos) (the "Click-Wrap" terms and conditions and "Contract"), which incorporates the Code.org Privacy Policy (at https://code.org/privacy). The Code.org Terms of Service are subject to the exceptions in Section 12.2 of this Addendum, and are superseded by the Addendum to the extent set forth in the preamble of this Addendum.

Denver Data Protection Agreement (Executed by Code.org)

Final Audit Report 2023-09-06

Created:	2023-09-06
By:	Melissa Haran (melissa_haran@dpsk12.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAATuI2zBAQOT8F20uV0GqMHk1Cc9fhAm3Z

"Denver Data Protection Agreement (Executed by Code.org)" History

Document digitally presigned by DocuSign\, Inc. (enterprisesupport@docusign.com)
2023-09-06 - 4:56:20 PM GMT

Document created by Melissa Haran (melissa_haran@dpsk12.org)
2023-09-06 - 7:09:56 PM GMT

Document emailed to Staci Crum (staci_crum@dpsk12.org) for signature
2023-09-06 - 7:11:09 PM GMT

Email viewed by Staci Crum (staci_crum@dpsk12.org)
2023-09-06 - 10:45:03 PM GMT

Document e-signed by Staci Crum (staci_crum@dpsk12.org)
Signature Date: 2023-09-06 - 10:45:47 PM GMT - Time Source: server

Agreement completed.
2023-09-06 - 10:45:47 PM GMT