GIRLS WHO CODE STUDENT DATA PRIVACY ADDENDUM

This Student Data Privacy Addendum ("**DPA**") is incorporated by reference into the Service Agreement (as defined below) entered into by and between the educational agency set forth below (hereinafter referred to as "**LEA**") and Girls Who Code (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 and LEA have entered into certain contractual documents (which collectively are referred to as the "**Service Agreement**"), to provide certain Services to the LEA as set forth in the Service Agreement and this DPA (collectively the "**Agreement**");

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

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

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

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

1. **Standard Schedule.** A description of the Service Agreement, and the categories of Student Data that may be processed by the Provider on behalf of LEA, and other information specific to this DPA are attached as **Exhibit "A" ("Standard Schedule").**

2. **Services.** The digital educational services and any other products and services that Provider may provide now or in the future to LEA pursuant to the Agreement (the "**Services**") as set forth in the Standard Schedule.

3. **Standard Clauses.** The Student Data Protection Clauses ("**Standard Clauses**") [1] attached hereto as **Exhibit "B"** are hereby incorporated by reference into this DPA in their entirety.

4. **Priority of Agreements.** With respect to the treatment of Student Data only, in the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy, the terms of this DPA shall control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect, including, without limitation, any license rights, limitation of liability or indemnification provisions.

5. **Term and Termination.** This DPA shall stay in effect for three (3) years, unless and until the extent terminated by the Parties. In the event that either Party seeks to terminate this DPA, they may do so by written notice so long as the Service Agreement has lapsed or been terminated. Either party may terminate this DPA and the Service Agreement if the other party breaches any material terms of this DPA.

6. **Effect of Termination**. If the Service Agreement is terminated, the Provider shall dispose of or return all of

[1] Modeled after the Student Data Privacy Consortium's (SDPC) National Student Data Privacy Model Clauses with changes to reflect how the Service operates.

LEA's Student Data pursuant to Article IV, Section 5 of the Standard Clauses.

7. **Notices**. All notices or other communication required or permitted to be given hereunder must be made in writing and may be given via e-mail transmission, or first-class mail, sent to the designated representatives set forth in the Standard Schedule.

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

9. **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.

10. **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 OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

11. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA ("**Change of Control**"), the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of such Change of Control. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

12. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

13. **Electronic Signature**: The Parties understand and agree that they have the right to execute this Agreement

through paper or through electronic signature technology, which is in compliance with applicable state and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of their electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Signatory Information

By signing below, I accept this DPA on behalf of the LEA. I represent and warrant that (a) I have full legal authority to bind the LEA to this DPA, (b) I have read and understand this DPA, and (c) I agree to all terms and conditions of this DPA on behalf of the LEA that I represent.

Name of LEA: _____

Address: _____

Country: _____

LEA Authorized Representative full name: _____

Title: _____

Email: _____

LEA Authorized Representative signature: _____

Date: _____

Girls Who Code Representative signature: _____

Authorized Representative full name: _____

Title: _____

Email: legal@girlswhocode.com

Address: Attn: Sarah Goldberg
Girls Who Code, Inc.
1250 Broadway, Floor 17
New York, New York 10001

Date: _____

EXHIBIT A DESCRIPTION OF SERVICES AND SERVICE AGREEMENT

1. **Service Agreements:** The Service Agreements include the Partnership Agreement (outlining specific programming for the LEA) and the Girls Who Code Terms of Service (entered into by all individual users of the LEA) as well as the Girls Who Code Clubs Privacy Policy and Clubs Children's Privacy Policy, located within the Girls Who Code Clubs Data Privacy Center, located here: https://hq.girlswhocode.com/privacy. The Club Terms of Service is located here: https://hq.girlswhocode.com/terms.

2. **Services:**

   2.1 Girls Who Code School Clubs: Girls Who Code Clubs provides free computer science programs, activities, and curriculum to school districts, library networks and afterschool programs for school aged students (each, a "**School Club**"). As a supplement to the program, Girls Who Code will provide access to its proprietary web-based headquarters platform to the School Club and their licensed users (the "**HQ Platform**") through accounts specifically created for and limited to students (**"Club Students"**), parents (**"Club Parents"**), teacher facilitators (**"Teacher Facilitators"**), and or school administrations supporting the School Club ("**School Club Administrators**") at School Clubs. The HQ Platform is designed to connect club stakeholders (Club Students, Teacher Facilitators, School Club Administrators, and Club Parents, respectively, collectively "**School Club Participants**") with School Club programming. The Services include:

   - Opportunities for Teacher Facilitators to provide feedback to Club Students; Club Students may use Clubs-HQ to ask and answer questions about their curricular activities, which will be visible to the Club Student, their Club Parent, their Teacher Facilitator and School Club Administrators.

   - Option for Club Students to post projects on the Project Gallery (within the HQ Platform, which requires credentials), which are visible to any user logged into Clubs-HQ, including other Club Students, Teacher Facilitators, School Club Administrators, and parents. (but not the general public).

   - Option for Club Students to interact with a messaging board that is visible to other Club Students in their Club, as well as their parent, and the Teacher Facilitator and School Club Administrators at their School.

   - Option (if selected by Teacher Facilitator) to engage with additional free digital resources (such as curriculum from Girls Who Code partners, access to interviews and insights from leaders in the technology, field, etc.) School Club Participants can access the learning resources, and leverage tools within the HQ Platform to run and participate in their School Club.

   - Additionally, the Services may utilize certain Third-Party Platforms as defined and set forth in the Service Agreement.

GWC never posts or shares a Club Student's Personal Information or Student Data publicly. Club Student Data in a Club Student's profile will only be visible to the Club Student, their Club Parent, their Teacher Facilitator, and their School Club Administrator at their School.

The Services include sharing Student Data with (i) authorized users of the Services, including parents or legal guardians and (ii) to protect the safety or integrity of users or others, or the security of the Services.

More information on how the Service operates is located at https://girlswhocode.com/programs/clubs-program.

Provider may also use De-Identified Data for educational research purposes, including transferring or sharing with third parties for such purposes.

2.2 Outside School Accounts and Outside School Programming:

The Services shall not include any Outside School Accounts or Outside School Programming. Club Students, Club Parents, and family users may have personal or non-school accounts (i.e., for use of the Girls Who Code program at home not related to school) in addition to School Club Accounts, this includes without limitation those accounts used in connection with Provider's Outside School Programming ("**Outside School Account(s)**"). An Outside School Account of a Club Student may also be linked to their Club Student account. Student Data shall not include information a student, parent, or family provides to Provider through such Outside School Accounts independent of the student's, parent's or family's engagement with the Services at the direction of the LEA.

"**Outside School Programming**" shall mean programming that children, parents, family users, and/or facilitators (all not connected to a school) may participate in not related to school use, including the Girls Who Code Summer Immersion Program ("SIP"), the Self-Paced Program ("SPP"), the College and Careers Programs, and the Code at Home program.

2.3 Additional opportunities for School Club Students: Girls Who Code provides additional opportunities for Club Students, including special events, workshops, contests, and Outside School Programming and may use Student Data as set forth in the Agreement (as modified by Ex. H) to send Program Communications (as defined in Ex. H) to School Club Participants about these additional opportunities.

3. Notices: In the event a written notice is to be provided pursuant to the DPA, notice shall be provided to the following recipients:

Notices to Provider
Feargus Leggett, CFO
1250 Broadway, Floor 17
New York, NY 10001
feargus.leggett@girlswhocode.com

With a copy to (if provided):

Notices to LEA
[LEA Name] _____
[LEA Mailing Address] _____
_____
[LEA E-mail Address] _____

With a copy to (if provided):

Sarah Goldberg
1250 Broadway, Floor 17
New York, NY 10001
legal@girlswhocode.com

[LEA Legal Counsel] _____
[LEA Legal Counsel Address] _____
_____
[LEA E-mail Address] _____

4. **Student Data Security Inquiries Contact**:

Provider
Sarah Goldberg
(917) 344-9523
legal@girlswhocode.com

LEA
[Name] _____
[Phone Number] _____
[E-mail Address] _____

5. **LEA Contact for Parent Inquiries Pursuant to Section 2.2:**

Sarah Goldberg
(917) 344-9523
legal@girlswhocode.com

6. **Disposition of Data:** Upon termination of the Agreement, Girls Who Code shall, unless directed otherwise by LEA, dispose of or delete Student Data obtained under the Service Agreement, within sixty (60) days of the date of termination (unless otherwise required by law). If the Agreement has lapsed or is not terminated, the Student Data shall be deleted at the earliest of (a) Girls Who Code's standard destruction schedule (located as part of the Clubs Data Retention Policy located on the Girls Who Code website Clubs Data Privacy Center), if applicable; (b) when the Student Data is no longer needed for the purpose for which it was received; or (c) as otherwise required by law. The duty to dispose or delete shall not extend to Student-Generated content that has been transferred or kept pursuant to Article II, Section 3. Girls Who Code may requested the LEA to provide special instructions for the treatment of Student Data through the "Directive for Disposition of Data form.

EXHIBIT

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.	☑
	Other application technology meta data-Please specify: click paths, reffering urls, access times, browser type, ISP, Page Views of logged in user, time spent on site, clicks of logged in users, engagement time of user	☑
Application Use Statistics	Meta data on user interaction with application	☑
Assessment	Standardized test scores	☐
	Observation data	☑
	Other assessment data-Please specify: Student work, Student generated content, Open text feedback providing feedback to student, anonymous student surveys	☑
Attendance	Student school (daily) attendance data	☐
	Student class attendance data	☐
Communications	Online communications captured (emails, blog entries)	☑
Conduct	Conduct or behavioral data	☐
Demographics	Date of Birth	☑
	Place of Birth	☐
	Gender	☐
	Ethnicity or race	☑
	Language information (native, or primary language spoken by student)	☑
	Other demographic information-Please specify: Low income status or economically disadvantaged status	☑
Enrollment	Student school enrollment	☑
	Student grade level	☑
	Homeroom	☐
	Guidance counselor	☐
	Specific curriculum programs	☐
	Year of graduation	☐
	Other enrollment information-Please specify:	☐
Parent/Guardian Contact Information	Address	☐
	Email	☑
	Phone	☐

Category of Data	Elements	Check if Used by Your System
Parent/Guardian ID	Parent ID number (created to link parents to students)	☑
Parent/Guardian Name	First and/or Last	☑
Schedule	Student scheduled courses	☐
	Teacher names	☐
Special Indicator	English language learner information	☑
	Low income status	☑
	Medical alerts/ health data	☐
	Student disability information	☐
	Specialized education services (IEP or 504)	☐
	Living situations (homeless/foster care)	☐
	Other indicator information-Please specify: Race and ethnicity / And ELL only when translation is requested by Student	☑
Student Contact Information	Address	☐
	Email	☑
	Phone	☐
Student Identifiers	Local (School district) ID number	☑
	State ID number	☐
	Provider/App assigned student ID number	☑
	Student app username	☑
	Student app passwords	☑
Student Name	First and/or Last	☑
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	☑
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	☐
Student Survey Responses	Student responses to surveys or questionnaires	☑
Student work	Student generated content; writing, pictures, etc.	☑
	Other student work data -Please specify: Photographs, videos or audio files- To customize their HQ account, to display an image in the project gallery, to communicate with other members of their school/program.	☑
Transcript	Student course grades	☐
	Student course data	☑
	Student course grades/ performance scores	☐

Category of Data	Elements	Check if Used by Your System
	Other transcript data - Please specify:	☐
Transportation	Student bus assignment	☐
	Student pick up and/or drop off location	☐
	Student bus card ID number	☐
	Other transportation data – Please specify:	☐
Other	Please list each additional data element used, stored, or collected by your application: **Please see the Information Transparency Chart located at https://girlswhocode.com/assets/downloads/craft-prod /downloads/Clubs-Data-Processing-Chart.pdf for additional details on: - Categories of Student Data - Categories of Data Subjects the Student Data is collected from and the source of the Student Data - Nature and purpose of the Processions activities of the Student Data The current list of Service Providers is located at https://girlswhocode.com/assets/downloads /craft-prod/downloads/Clubs-Third-Party-Providers.p	☑
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

EXHIBIT B
STANDARD CLAUSES

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, including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

1.2 DPA Definitions. The definition of terms used in this DPA are found in **Exhibit "C".** With respect to the treatment of Student Data, in the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

1.3 Exemptions under FERPA. LEA may not generally disclose Personally Identifiable Information from an eligible student's Educational 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 the School Official exemption ("**School Official Exemption**"). For the purposes of FERPA, to the extent Personally Identifiable Information from Educational 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 with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the control and direction of the LEAs, with respect to Educational Records and Student Data. Additionally, at the election of LEA, certain information provided to Provider by LEA about a student, such as student name and grade level, may be considered Directory Information under FERPA and thus not subject to the restrictions for Educational Records.

2. DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1 Student Data Property of LEA. As between LEA and Provider, all Student Data processed by the Provider pursuant to the Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA or the party who provided such data (such as the student or parent).

2.2 Parent Access. To the extent required by law, the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Educational Records and/or Student Data, correct erroneous information, and procedures for the transfer of Student-Generated Content to a personal account, consistent with the functionality of the Services. If LEA is not able to update the Student Data itself, Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in an Educational Record held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information, provided however, that Provider may also allow for direct access requests (but not correction or deletion rights) of Student Data and/or Educational Records from a verified parent.

2.3 **Separate Account and Student Generated Content**. Students, parents and family users may have personal or non-school accounts (i.e. for use of Girls Who Code at home not related to school) in addition to school accounts, this includes, without limitation, those accounts used in connection with Provider's Outside School Programming (as defined on Exhibit A) ("**Outside School Account(s)**"). An Outside School Account of a student may also be linked to their student account. Student Data shall not include information a student, parent or family provides to Provider through such Outside School Accounts independent of the student's, parent's or family'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 and to the extent consistent with law, Provider may provide a reasonable mechanism through which the LEA, eligible student, or the student's parent or legal guardian, may download, export, transfer, or otherwise save or maintain the Student Generated Content to a separate student account or the Outside School Account upon termination of the Service Agreement; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service.

2.4 **Third Party Requests**. Should a third party, excluding a Service Provider, including, but not limited to, law enforcement or other government entities ("**Requesting Party(ies)**") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall redirect the Requesting Party to request the Student Data directly from the LEA and shall not provide the requested Student Data to the Requesting Party, unless and to the extent that Provider reasonably believes it is compelled to 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 the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request or otherwise legally prohibited.

2.5 **Service Providers**. Provider shall enter into written agreements with all Service Providers performing functions for the Provider in order for the Provider to provide the Services pursuant to the Agreement, whereby the Service Providers agree to protect Student Data in a 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 Applicable Laws**. LEA shall use the Services for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

3.2 **Annual Notification of Rights**. If the LEA has a policy of disclosing Educational Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of FERPA rights ("**Annual Notification of Rights**"). Additionally, LEA represents, warrants and covenants to Provider, as applicable, that LEA has:

- **a.** Complied with the School Official Exemption, including, without limitation, informing parents in their Annual Notification of Rights that the LEA defines "school official" to include service providers such as Provider and defines "legitimate educational interest" to include services such as the type provided by Provider; and/or
- **b.** 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

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.

3.3 **Reasonable Precautions**. LEA shall employ administrative, physical and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted data from unauthorized access, disclosure or acquisition by an unauthorized person.

3.4 **Unauthorized Access Notification**. LEA shall notify Provider promptly, but in no event 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 with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security applicable to the Provider in providing the Service to the LEA, all as may be amended from time to time.

4.2 **Authorized Use.** The Student Data shared pursuant to the Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under law.

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

4.4 **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this Agreement. This prohibition against disclosure shall not apply to (i) De-Identified information, (ii) Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, (iii) to Service Providers performing services on behalf of the Provider pursuant to this DPA, (iv) to authorized users of the Services, including parents or legal guardians, or (v) to protect the safety or integrity of users or others, or the security of the Services. Provider will not Sell Student Data to any third party.

4.5 **De-Identified Data.** Provider agrees not to attempt to re-identify De-Identified Student Data without the written direction of the LEA. De-Identified Student Data may be used by the Provider for those purposes allowed under FERPA and applicable state student privacy laws, as well as the following purposes (1) assisting the LEA or other governmental agencies in conducting research and other studies; (2) research, development, and improvement of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Provider agrees not to transfer De-identified Student Data to any third party unless that party agrees in writing not to attempt re-identification. Prior to publishing any document that names the LEA, the Provider shall obtain the LEA's written approval of the manner in which

De-Identified Student Data is presented.

4.6 **Disposition of Data**. Upon termination of the Agreement, the Provider shall, unless directed otherwise by LEA, dispose of or delete Student Data obtained under the Agreement, within sixty (60) days of the date of termination (unless otherwise required by law). If the Agreement has lapsed or is not terminated, the Student Data shall be deleted at the earliest of (a) Provider's standard destruction schedule, if applicable; (b) when the Student Data is no longer needed for the purpose for which it was received; or (c) as otherwise required by law. The duty to dispose of or delete Student Data shall not extend to Student Data that has been De-Identified or to Student-Generated Content that has been transferred or kept pursuant to Section 2.3. The LEA may provide the Provider with special instructions for the treatment of Student Data, by transmitting to Provider the "**Directive for Disposition of Data**" form, a copy of which is attached hereto as **Exhibit "D"**.

4.7 **Advertising Limitations.** Provider is prohibited from using, disclosing, or Selling Student Data (a) to inform, influence, or enable Targeted Advertising; (b) to develop a profile of a student, for any purpose other than providing the Service to LEA, or as authorized by the parent or legal guardian; or (c) for any commercial purpose other than to provide the Service to the LEA, as authorized by the LEA or the parent/guardian, or as permitted by applicable law. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations or sending Program Communications to account holders); or (ii) to make product recommendations to teachers, LEA employees, or parents/legal guardians; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

5. DATA SECURITY AND BREACH PROVISIONS

5.1 **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

5.2 **Audits.** No more than once per contract year, or following a Security Incident, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit at LEA's expense, during normal business hours and at a time convenient for the Provider, the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of Services to the LEA ("**Security Audit**"). In connection with any Security Audit, the Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA, as reasonably necessary to fulfill the requests of such Security Audit. Alternatively, Provider may provide an independent third-party report in place of allowing LEA to conduct such Security Audit.

5.3 **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "E"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "E"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

5.4 **Data Breach**. In the event that Provider confirms an unauthorized release, disclosure of, or access to Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider in violation of applicable state or federal law (a "**Security Incident**"), the Provider shall provide notification

to LEA as required by the applicable state law, but in no event later than seventy-two (72) hours of confirmation of the Security Incident ("**Security Incident Notification**"), unless notification within this time limit would disrupt investigation of the incident, by either the Provider or by law enforcement. In such an event, the Security Incident Notification shall be made within a reasonable time after the discovery of the Security Incident. A Security Incident does not include the good faith acquisition of Student Data by an employee or agent of Provider for a legitimate purpose, provided that the Student Data is not used for a purpose unrelated to the Provider's Service or subject to further unauthorized disclosure. Provider shall follow the following process:

5.4.1 Unless otherwise required by applicable state law, the Security Incident Notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

1. The name and contact information of the reporting Provider subject to this section.
2. A list of the types of PII that were or are reasonably believed to have been the subject of the Security Incident.
3. If the information is possible to determine at the time the notice is provided, then either (a) the date of the Security Incident, (b) the estimated date of the Security Incident, or (c) the date range within which the Security Incident occurred. The Security Incident Notification shall also include the date of the Security Incident Notice.
4. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
5. A general description of the Security Incident, if that information is possible to determine and legally permissible to provide at the time the Security Incident Notification is provided.

5.4.2 Provider agrees to adhere to all requirements applicable to Provider providing the Services in applicable federal and state 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.

5.4.3 Provider further acknowledges and agrees to have a written incident response plan that 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 summary of said written Incident Response Plan.

5.4.4 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. LEA shall provide notice and facts surrounding the Security incident to the affected students, parents or guardians. 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.

5.4.5 In the event of a Security Incident originating from LEA's actions or use of the Service, or otherwise a result of LEA's actions or inactions ("**LEA Security Incident**"), Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data and may request from LEA reasonable costs incurred as a result of the LEA Security Incident.

EXHIBIT "C"

DEFINITIONS

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

Educational Records: Educational Records shall have the meaning 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.

Personally Identifiable Information, Personal 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. summer programming) offered through the Services or Girls Who Code website or application.

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

"Sell" consistent with the Student Privacy Pledge, does not include or apply to a Change of Control, 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 storing, sharing, transferring or disclosing Student Data with a Service Provider 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 (i) if a user directs Provider to intentionally disclose Student Data or uses the Service to intentionally interact with a third party, provided that such third party also does not Sell the Student Data; or (ii) if a parent or a third party authorized by the parent lawfully acquires Student Data (e.g., enhanced classroom reports or photos) for fee or for a fee.

Service Provider: For the purposes of this DPA, the term "Service Provider" means a party other than LEA or Provider, with whom Provider has a written agreement as set forth in the Standard Clauses, Section 2.5, and who Provider uses for data collection, analytics, storage, or other service necessary to operate and/or improve its service, and who has access to or storage of Student Data.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the Services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files,

photographs, videos, and account information that enables ongoing ownership of student content.

Student Data: Student Data includes any Personally Identifiable Information, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, 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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, or any other information or identification number that would provide information about a specific student. Student Data further includes Personally Identifiable Information, as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Educational Records are Student Data for the purposes of this DPA. Student Data as specified in **Exhibit "B"** in the Standard Schedule is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not include i) De-Identified Data or information that has been anonymized, or anonymous usage data regarding a student's or LEA's use of Provider's Services or ii) any data collected from an Outside School Account, including, without, limitation, through Provider's Outside School Programing.

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

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF STUDENT DATA

LEA directs Provider 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 Student 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 as set forth in Section 4.6 ("Disposition of Data"). De-Identification of Student Data shall be deemed a destruction or deletion.

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

[Insert or attach special instructions]

3. Timing of Disposition

Student Data shall be disposed of by the following date:

__ As soon as commercially practicable

__By *[Insert Date]*

4. Signature

_____
Authorized Representative of LEA

_____
Date

5. Verification of Disposition of Data

_____
Authorized Representative of Company

_____
Date

EXHIBIT "E"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

Cybersecurity Frameworks

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

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

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

Additionally, the Girls Who Code Security White Paper can be found here: https://girlswhocode.com/assets/ downloads/craft-prod/downloads/GWC-Security-Whitepaper-1.pdf