

STANDARD STUDENT DATA PRIVACY AGREEMENT

TX-NDPA v1r6

School District or LEA

NORTHSIDE ISD

and

Provider

Code.org

STANDARD STUDENT DATA PRIVACY AGREEMENT

TX-NDPA

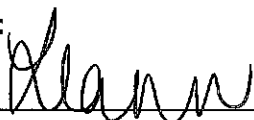
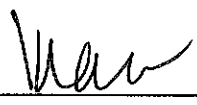
The designated representative for the LEA for this DPA is:

Name: LEANN KIDD Title: EXECUTIVE DIRECTOR OF TECHNOLOGY SERVICES
 Address: 5734 FARINON DIRVE SAN ANTONIO, TEXAS
 Phone: 2103977200 Email: LEANN.KIDD@NISD.NET

The designated representative for the Provider for this DPA is:

Name: Cameron Wilson Title: President
 Address: 801 Fifth Ave, #2100, Seattle WA 98104
 Phone: (206) 420-1376 Email: cameron@code.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA:
 By:   Date: 9-24-25

Printed Name: LEANN KIDD Title/Position: EXECUTIVE DIRECTOR OF TECHNOLOGY SERVICES

Provider:

By:  Signed by: DB0384E853DF436... Date: 9/17/2025 | 04:41:47 PDT

Printed Name: Cameron Wilson Title/Position: President

3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the 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.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data 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.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education 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 rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

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, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
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

ARTICLE V: DATA PROVISIONS

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.
2. **Audits.** No more than once a year, or following unauthorized access, 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 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. 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. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
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 "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall 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.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

Exhibit "H", the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **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.
5. **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.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, 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.
7. **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, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the 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.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

EXHIBIT "A"**DESCRIPTION OF SERVICES**

Code.org® is a nonprofit dedicated to expanding access to computer science in schools and increasing participation by young women and students from other underrepresented groups. Its vision is that every student in every school has the opportunity to learn computer science as part of their core K-12 education. As part of its 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 and to display and share their work subject to the Code.org Terms of Services ([athttps://code.org/tos](https://code.org/tos)) (the Service Agreement), which incorporates the Code.org Privacy Policy ([athttps://code.org/privacy](https://code.org/privacy)).

The Code.org online curriculum and learning platform 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 for both purposes. If a student or parent creates a personal login for a Code.org account (using an email address and password), 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, subject to the process outlined in the following paragraph, the student's Code.org account (and the Student Generated Content associated with the account) will not be deleted when a teacher's account is deleted - both the student and LEA would need to request deletion. Conversely, as long as the student remains part of a teacher's section, the student cannot delete the account without asking the teacher to 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. For purposes of Article II, Section 3 of the NDPA, there is no "separate account." However, this personal login feature provides the mechanism by which the student can maintain Student-Generated Content.

Notwithstanding the foregoing, if the LEA wishes to ensure the deletion of all Code.org student accounts enrolled in an LEA's teacher's section (i.e., including those student accounts using a personal login), Code.org will do so based on an LEA's specific request made to privacy@code.org. This process requires that the LEA either (1) identify each teacher account with sections the LEA seeks to delete so that Code.org can identify student accounts enrolled in those teacher's sections (note: 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 an LEA email address domain was used to establish the personal login) or (2) ask that Code.org identify all teacher accounts using a specific LEA 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 all student accounts in those sections along with all student-generated content associated with those accounts. The LEA is responsible for warning 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 LEA.

STANDARD STUDENT DATA PRIVACY AGREEMENT

TX-NDPA

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify: Age – not Date of Birth	<input checked="" type="checkbox"/>
Enrollment	Student school enrollment	<input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input checked="" type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>

STANDARD STUDENT DATA PRIVACY AGREEMENT

TX-NDPA

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/ performance scores	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>
Other	Please list each additional data element used, stored, or collected by your application:	<input type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

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

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

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "E"**GENERAL OFFER OF PRIVACY TERMS****1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and [NORTHSIDE ISD] ("Originating LEA") which is dated [], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: _____

[NAME OF PROVIDER]

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the [Insert Name of Originating LEA] and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

Subscribing LEA:

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____ Title: _____

Address: _____

Telephone Number: _____ Email: _____

EXHIBIT "G"**Supplemental SDPC State Terms for Texas**

Version 1.0

This **Exhibit "G"**, Supplemental SDPC State Terms for Texas ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between [NORTHSIDE ISD] (the "Local Education Agency" or "LEA") and [Code.org] (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Covered Data.** All instances of "Student Data" should be replaced with "LEA Data". The protections provided within this DPA extend to all data provided to or collected by the Provider.
2. **Compliance with Texas Privacy Laws and Regulations.** In performing their respective obligations under the Agreement, the LEA and the Provider shall comply with all Texas laws and regulations pertaining to LEA data privacy and confidentiality, including but not limited to the Texas Education Code Chapter 32, and Texas Government Code Chapter 560.
3. **Modification to Article III, Section 2 of the DPA.** Article III, Section 2 of the DPA (Annual Notification of Rights.) is amended as follows:

Annual Notification of Rights. ~~If the LEA has a policy of disclosing Education 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 rights.~~

Consider Provider as School Official. The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records received from the LEA pursuant to the DPA. For purposes of the Service Agreement and this DPA, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from the education records received from the LEA.

4. **Modification to Article V, Section 4 of the DPA.** Article V, Section 4 of the DPA (Data Breach.) is amended with the following additions: (6) For purposes of defining an unauthorized disclosure or security breach, this definition specifically includes meanings assigned by Texas law, including applicable provisions in the Texas Education Code and Texas Business and Commerce Code. (7) The LEA may immediately terminate the Service Agreement if the LEA determines the Provider has breached a material term of this DPA. (8) The Provider's obligations shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

EXHIBIT "H"

ADDITIONAL TERMS OR MODIFICATIONS

LEA and Provider agree to the following additional terms and modifications: The following sections shall be modified (as indicated) and replaced with the language set forth below.

1. Agreement Section 4 - Term

This DPA shall stay in effect for three (3) years, unless earlier terminated as set forth herein. Exhibit E will expire three (3) years from the date the original DPA was signed, unless earlier terminated as set forth herein.

2. Article I, Section 2

Student Data to Be Provided. In order to perform the Services described above, the Student Data processed by Provider on behalf of LEA shall provide Student Data as be identified in the Schedule of Data, attached hereto as Exhibit "B".

3. Article IV, Section 1

Privacy Compliance. The Provider shall comply, in all material respects, with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time, applicable to the Provider in providing the Service to LEA.

4. Article IV, Section 2

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

5. Article IV, Section 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 DPA. This prohibition against disclosure shall not apply to ~~aggregate summaries of De-Identified Data information,~~ Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, ~~or to subprocessors performing services on behalf of the Provider pursuant to this DPA, or to protect the safety of users or others or the security of the Services.~~ Provider will not Sell Student Data to any third party.

6. Article IV, Section 5

De-Identified Data: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; ~~and~~ (2) research and development 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

10. Exhibit G – Supplemental SDPC State Terms for Texas

5. **Modification to Article VII, Section 4 of the DPA.** Article ~~VII~~ VI, Section 4 of the DPA (Entire Agreement ~~Annual Notification of Rights~~.) is amended as follows:

Entire Agreement. This DPA ~~and the Service Agreement~~ constitutes the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

6. **Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach (as described in Article V, Section 4) that is attributable to the Provider (i.e., caused by Provider's actions or inactions), the Provider shall reimburse and indemnify the LEA for reasonable ~~any and all~~ costs and expenses that the LEA incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with:

- a. Providing notification to the employees or parents of those students whose LEA Data was compromised and regulatory agencies or other entities as required by law or contract;
- b. ~~Providing credit monitoring to those employees or students whose LEA Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the employee's or student's credit or financial security;~~
- c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and
- d. Providing any other notifications or fulfilling any other requirements adopted by the Texas State Board of Education, Texas Education Agency, or under other State or federal laws.