STUDENT DATA PRIVACY AGREEMENT
VERSION (2019)

Wayland Public Schools

and

Code.org

June 11, 2020

This Student Data Privacy Agreement ("DPA") is entered into by and between the school district, Wayland Public Schools (hereinafter referred to as "LEA") and Code.org (hereinafter referred to as "Provider") on June 11, 2020. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") as described in Article I and Exhibit "A"; and

WHEREAS, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts who are part of The Education Collaborative's ("TEC") services in Massachusetts, New Hampshire, and Rhode Island the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, including, but not limited to, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws depending on the state in which the Services are provided. Specifically, those laws are: in Massachusetts: 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; in New Hampshire: RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; in Rhode Island: R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.;;

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

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

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data and Teacher Data (as defined in Exhibit "C") transmitted to Provider from the LEA pursuant to Exhibit "A", including compliance with all applicable Federal and state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, in Massachusetts: 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; in New Hampshire: RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; in Rhode Island: R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.;; and other applicable state laws, all as may be amended from time to time. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit "C") from Pupil Records (as defined in Exhibit "C") and Teacher Data are transmitted to Provider from 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 direct control and supervision of the LEA with respect to the use and maintenance of Student Data and Teacher Data.

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

3. **Student Data to Be Provided**. In order to perform the Services described in this Article and Exhibit "A", LEA shall provide the categories of Student Data and Teacher Data described in the Schedule of Data, attached hereto as Exhibit "B".

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data or Teacher Data transmitted to the Provider pursuant to this 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 or Teacher 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 Agreement in the same manner as the original Student Data or Teacher Data. The Parties agree that as between them all rights, including all intellectual property rights in and to Student Data or Teacher Data contemplated per this Agreement shall remain the exclusive property of the LEA.

2. **Exemptions under FERPA.** For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data and Teacher Data notwithstanding the above. The Provider will cooperate and provide Student Data and Teacher Data within ten (10) days at the LEA's request. Provider may transfer Pupil-Generated Content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the Pupil's Records, correct erroneous information, and procedures for the transfer of Pupil-Generated Content to a personal account, consistent with the functionality of services. Provider shall cooperate and respond within ten (10) days to the LEA's request for PII in a Pupil's Records held by the Provider to view or correct as necessary. The Provider will cooperate and respond without unnecessary delay for Student Data related to special education students and, for such requests made in anticipation of an IEP meeting, due process hearing, or resolution session, without unnecessary delay and before any such meeting, due process hearing, or resolution session and, in either case, in no event more than ten (10) days from the date of the request to the LEA's request for Student Data in a Pupil's Records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of 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.

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

4. **Third Party Request**. Should a Third Party, excluding a Subprocessor, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for Student Data or Teacher Data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA, unless and to the extent that Provider reasonably believes it must grant such access to the third party because the data disclosure is necessary: (i) pursuant to a court order or legal process, or (ii) to comply with statutes or regulations, and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data or Teacher Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data, Teacher Data, and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data or Teacher Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student or teacher's use of Provider's services.

5. **No Unauthorized Use**. Provider shall not use Student Data, Teacher Data, or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.

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

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws**. LEA shall provide Student Data and Teacher Data for the purposes of the DPA in compliance with any applicable state or federal laws and regulations pertaining to data privacy and security, including without limitation the FERPA, PPRA, IDEA, and in Massachusetts: 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; in New Hampshire: RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; in Rhode Island: R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."

2. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

3. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or

suspected unauthorized use or access of the Services, LEA's account, Student Data, or Teacher Data. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply in all material respects with all applicable state and federal laws and regulations pertaining to data privacy and security, applicable to the Provider in providing the Service to LEA. With respect to Student Data that the LEA permits Provider to collect or access pursuant to the Agreement, including FERPA, COPPA, PPRA, in Massachusetts: 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; in New Hampshire: RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; in Rhode Island: R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and all other applicable privacy statutes and regulations.

4. **Authorized Use**. Student Data and Teacher Data shared pursuant to this DPA shall be used for no purpose other than the Services stated in this DPA and/or otherwise legally required, including without limitation, for adaptive learning or customized student learning. The foregoing limitation does not apply to any De-identified Data. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data, Teacher Data, or any portion thereof without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 5, or there is a court order or lawfully issued subpoena for the information or such disclosure is authorized under the statutes referred to in subsection (1), above.

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

5. **De-identified Data**. De-identified Data, as defined in Exhibit "C", may be used by the Provider for any lawful purpose, including without limitation the purposes of development and improvement of educational sites, services, or applications. Provider may share De-identified Student and Teacher Data with third party researchers operating under a Data Sharing Agreement for the non-commercial purposes of broadening the educational knowledge base about how Computer Science education impacts elementary and secondary student learning and demonstrating the effectiveness of the Services. These third party researchers are bound by a mutually executed Data Sharing Agreement to the same level of care as Provider with regards to the treatment, usage, return and destruction of De-identified Student and Teacher Data. As part

of these data sharing agreements, these third party researchers agree in writing not to attempt re-dentification. These third party researchers include:

- Stanford University
- MIT
- Harvard
- Raleigh Technical Institute
- West Coast Analytics
- American Institutes of Research
- University of Rhode Island
- Washington University (St. Louis)
- University of Washington
- SageFox Consulting
- Carnegie Mellon
- North Carolina State
- University of Maryland

Provider's use of such De-identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Provider agrees not to attempt to re-identify de-identified Student Data and Teacher Data and not to transfer de-identified Student Data and Teacher Data to any other party unless a) that party agrees in writing not to attempt re-identification., and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data**. In accordance with the applicable terms in subsection (a) or (b) below, and upon a written request from the LEA, Provider shall dispose or delete all Student Data and Teacher Data under the DPA within thirty (30) days of the date of receipt of such written request. If no written request is received, Provider shall dispose or delete all Personally Identifiable Information contained in Student Data at the earliest of (a) when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law. Nothing in the DPA authorizes Provider to maintain PII or Teacher Data obtained under any other writing beyond the time period reasonably needed to complete the disposition unless a student, parent or legal guardian of a student chooses to establish a separate contractual relationship with the Provider and provides written consent for the transfer of the Student Data. Disposition shall include (1) the shredding of any hard copies of any Student Data and Teacher Data; (2) Erasing any Personally Identifiable Information; or (3) Otherwise modifying the Personally Identifiable Information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Student Data and Teacher Data has been disposed. Upon receipt of a request from the LEA, the Provider will also immediately provide the LEA with any specified portion of the Student Data or Teacher Data within ten (10) calendar days of receipt of said request. The LEA may also employ a "Request for Return or Deletion of Student Data" FORM, a Copy of which is attached hereto as Exhibit "D") for the written request.

(a) **Partial Disposal During Term DPA.** Throughout the Term of this DPA, LEA may request in writing partial or complete disposal of Student Data or Teacher Data obtained the DPA. Partial or complete disposal of data shall occur within forty-five (45) days.

(b) **Complete Disposal Upon Termination.** Upon termination of the DPA, Provider shall dispose or delete all Student Data and Teacher Data obtained within forty-five (45) days.

7. **Advertising Prohibition**. Provider is prohibited from leasing, renting, using or selling Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA or as authorized by the parent or legal guardian pursuant to a separate written contract between the Provider and parent and legal guardian or LEA; or (c) use the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.

ARTICLE V: DATA SECURITY AND BREACH PROVISIONS

1. **Data Security**. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures. The Provider agrees to employ administrative, physical, and technical safeguards, consistent with industry standards and technology best practices, to protect Student Data and Teacher Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data and Teacher Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data and Teacher Data to employees or contractors that are performing the Services. Employees with access to Student Data and Teacher Data shall have signed confidentiality agreements regarding said Student Data and Teacher Data. All employees with access to Student Data and Teacher Data shall pass criminal background checks.

   b. **Destruction of Data**. Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and Teacher Data and obtained under the DPA according to the procedure identified in Article IV, Section 5. Nothing in the DPA authorizes Provider to maintain PII or Teacher Data beyond the time period reasonably needed to complete the disposition.

   c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any Student Data or Teacher Data, including ensuring that Teacher or Student Data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Teacher Data and Student Data obtained or generated pursuant to the DPA in a secure computer environment and not copy, reproduce, or transmit Teacher Data and Student Data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA or as set forth in the agreement. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, Section 4.

d. Employee Training. The Provider shall provide recurring, periodic (no less than annual, with additional sessions as needed throughout the year to address relevant issues/changes, such as (but not necessarily limited to) new or evolving security threats, changes to security protocols or practices, changes to software and/or hardware, identified vulnerabilities, etc.) security training to those of its employees who operate or have access to the system. Such trainings must be tailored to the Provider's business and cover, but not necessarily be limited to, the following topics: common types of attackers (e.g., cyber criminals, hacktivists, government sponsored groups, inside threats, etc.); common types of attacks (e.g., social engineering, spoofing, phishing, etc.) and how the information sought is typically used; identifying threats, avoiding threats, physical security and environmental controls; internal policies and procedures; and safe internet habits. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. Security Technology. When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.

f. Security Coordinator. Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data and Teacher Data received pursuant to the DPA.

g. Subprocessors Bound. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data and Teacher Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

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

i. Backups. Provider agrees to maintain backup copies, backed up at least daily, of Student Data and Teacher Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data, Teacher Data, or any portion thereof.

j. Audits. At least once a year, except in the case of a verified breach, the Provider may, upon receipt of written request and with at least ten (10) business days advance notice, allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student Data or Teacher Data or any portion thereof, subject to reasonable time and manner restrictions. The Provider will cooperate reasonably with the LEA and any state or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students, teachers, and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and Teacher Data and all records pertaining to the Provider, LEA and delivery of Services to the Provider.

k. **Additional Data Security Requirements.** The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:

(1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;

(2) Limit unsuccessful logon attempts;

(3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;

(4) Authorize wireless access prior to allowing such connections;

(5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

(6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

(7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;

(8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

(9) Enforce a minimum password complexity and change of characters when new passwords are created;

(10) Perform maintenance on organizational systems;

(11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;

(12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;

(13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;

(14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

(15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;

(16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

(17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

(18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

(19) Protect the confidentiality of Student Data and Teacher Data at rest;

(20) Identify, report, and correct system flaws in a timely manner;

(21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

(22) Monitor system security alerts and advisories and take action in response; and

(23) Update malicious code protection mechanisms when new releases are available.

2. **<u>Data Breach</u>**. In the event that Provider becomes aware of any actual or reasonably suspected disclosure or access to Student Data or Teacher Data by an unauthorized individual, Provider shall provide notification to LEA as required by the applicable state law, but in no event later than thirty (30 days) following discovery of the Security Incident (each a "Security Breach Notification"). Unless otherwise required by the applicable law, the Security Breach Notification shall contain the following:

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

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

      i. The name and contact information of the reporting 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 the Security Incident.

      iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the Security Incident, (2) the estimated date of the breach, or

(3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether, to the knowledge of the Provider, the Security Breach Notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

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

vi. The estimated number of students and teachers affected by the Security Incident, if any.

vii. Information about what the Provider has done to protect individuals whose PII has been breached, including toll free numbers and websites to contact:

1. The credit reporting agencies
2. Remediation service providers
3. The attorney general

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

ix. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

c. Provider agrees to adhere to all requirements in the Data Breach laws of the applicable state where the LEA is located and in federal law with respect to a Security Incident related to the Student Data and Teacher Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data Security Incident.

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

e. At the request of the LEA, Provider shall assist the LEA in notifying the affected parent, legal guardian, staff member, or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) above.

ARTICLE VI: MISCELLANEOUS

1. Term. The Provider shall be bound by this DPA and any service agreement for three years. The DPA and any service agreement will automatically renew at the end of the term for one year at a time, unless either party gives written notice of the termination at least thirty days prior to the end of the relevant term.

2. **Termination**. The LEA may terminate this DPA and any service agreement at any time.

3. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall destroy all of LEA's Student Data and Teacher Data pursuant to Article V, section 1(b).

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA, IDEA. COPPA, PPRA, in Massachusetts: 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; in New Hampshire: RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; in Rhode Island: R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; With respect to Student Data and Teacher Data in the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.

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

   The designated representative for the Provider for this Agreement is:

Name ________________________
Title ________________________ Privacy Officer
Address ________________________ 1501 Fourth Avenue, Suite 900
Telephone Number ________________________ (206) 420-1476
Email __________________________privacy@code.org

The designated representative for the LEA for this Agreement is:

Name Leisha Simon
Title Director of Technology
Address 41 Cochituate Road, Wayland, MA 01778
Telephone Number 508.358.3714
Email HYPERLINK "mailto:leisha_simon@wayland.k12.ma.us"leisha_simon@wayland.k12.ma.us

6. **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.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

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

9. **Authority.** Both parties represent that they are authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data, Teacher Data, and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data, Teacher Data, and/or any portion thereof.

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

11. **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 the applicable state law 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.

Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason in writing.

If either party would like a paper copy of this Agreement, they may request a copy from the other party.

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

13. **Merger or Acquisition:** The Provider may assign to any successor through merger, sale or other disposal method its obligations and rights under this DPA. The Provider must require the successor to assume all obligations of this DPA. In the event that the Provider anticipates selling, merging or otherwise disposing of its business to a successor during the term of the DPA, the Provider shall provide written notice of the proposed sale, merger or disposal to the LEA no later than sixty (60) days prior to the anticipated date of sale, merger or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA. 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

ARTICLE VII- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit “E”), be bound by the terms of this to any other TEC school district who signs the acceptance in said Exhibit.

[*Signature Page Follows*]

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

WAYLAND PUBLIC SCHOOLS

By: Arthur Unobskey
Arthur Unobskey (Jun 14, 2020 10:09 EDT) Date: 6-14-20

Printed Name: Arthur Unobskey Title: Superintendent

CODE.ORG

By: Cameron Wilson Date: 6/12/2020

Printed Name: Cameron Wilson Title: COO

EXHIBIT “A”

DESCRIPTION OF SERVICES

Code.org, a learn-to-code application.

For the purposes of this Agreement, activities that save individual progress require an individual Student account in the Provider's online platform that is created by their Teacher as part of a class section of this LEA, and will form the basis for collection of Student and Teacher Data as defined in this Agreement.

Student accounts created by individual students or their parents that are not part of a Teacher-created class section of this LEA are excluded from this Agreement.

Activities which do not allow an individual account login and which do not save student progress are excluded from this Agreement.

EXHIBIT “B”

SCHEDULE OF STUDENT DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify: standard log files, web beacons, and pixel tags	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify: Student answers to assessments in Code.org coursework, individual lesson evaluation/grades	X
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, preferred or primary language spoken by student)	X
	Other demographic information-Please specify: Age	X
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	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	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	**Elements**	**Check if used by your system**
Student Contact Information	Address	
	Email (used temporarily to recover an account – not stored)	X
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Vendor/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	X

Category of Data	Elements	Check if used by your system
Student work	Student generated content; writing, pictures etc.	X
	Other student work data - Please specify: Projects and Code.org coursework	X
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	

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

SCHEDULE OF TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify: standard log files, web beacons, and pixel tags	X
Application Use Statistics	Meta data on user interaction with application	X
Communications	Online communications that are captured (emails, blog entries)	X
Demographics	Date of Birth	X
	Place of Birth	
	Social Security Number	
	Ethnicity or race	X
	Other demographic information-Please specify: Age	X
Personal Contact Information	Personal Address	X
	Personal Email	X
	Personal Phone	X
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	X
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	

Category of Data	Elements	Check if used by your system
Teacher Identifiers	Local (School district) ID number	X
	State ID number	X
	Vendor/App assigned teacher ID number	X
	Teacher app username	X
	Teacher app passwords	X
Teacher In App Performance	Program/application performance	X
Teacher Survey Responses	Teacher responses to surveys or questionnaires	X
Teacher work	Teacher generated content; writing, pictures etc.	X
	Other teacher work data - Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application. Teachers can choose to use all lessons/projects as students to try them out (in which case student level data is collected.) Additionally, teachers can choose to participate in additional services from Code.org such as teacher forums or Professional Learning.	X

EXHIBIT “C”

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information (“PII”) from Pupil records or Teacher Data in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students and staff. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student or staff member, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

NIST 800-63-3: Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, Student Data, Teacher Data, metadata, and user or Pupil-Generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, teachers, or students’ parents/guardians. PII includes, without limitation, at least the following:

First Name
Last Name
Telephone Number
Discipline Records
Special Education Data
Grades
Criminal Records
Health Records
Biometric Information
Socioeconomic Information
Political Affiliations
Text Messages
Student Identifiers
Photos
Videos
Grade
Place of birth
Unique pupil identifier

Home Address
Subject
Email Address
Test Results
Juvenile Dependency Records
Evaluations
Medical Records
Social Security Number
Disabilities
Food Purchases
Religious Information
Documents
Search Activity
Voice Recordings
Date of Birth
Classes
Social Media Address
Personal Biography

Credit card account number, insurance account number, and financial services account number
Name of the student’s parents or other family members, including mother’s maiden name
Attendance and mobility information between and within LEAs
Gender, Race, Ethnicity

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's or Staff member's Email

Information that is created by a student or the student's parent or provided to an employee or agent of the school, LEA, or the Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes

Information that is created or provided by an employee or agent of the school or LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes

Information that is gathered by a Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes

Teacher: It includes teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

Teacher Data: For the purposes of this DPA, it applies to teachers, paraprofessionals, principals, school employees, contractors, and other administrators. It includes at least the following:

Social security number.
Date of birth.
Personal street address.
Personal email address.
Personal telephone number
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Pupil Records/Teacher Records.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any PII that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

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

The definition of “school official” encompasses the definition of “authorized school personnel” under 603 CMR 23.02 for Massachusetts LEAs.

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, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number, student identifiers, search activity, photos, voice recordings, attendance and mobility information between and within LEAs, gender, race, ethnicity or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of State and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services.

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

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

Third Party: The term “Third Party” means an entity that is not the provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[Name or District or LEA] directs Code.org to dispose of data obtained by Company 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 data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

___ Disposition shall be by destruction or deletion of data.

___ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions.]

3. Timing of Disposition

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

OPTIONAL: EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy? □ Yes □ No

If yes, please provide it.

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

____ ISO 27001/27002

____ CIS Critical Security Controls

____ NIST Framework for Improving Critical Infrastructure Security

____ Other: ____

3. Does your organization store any customer data outside the United States? □ Yes □ No

4. Does your organization encrypt customer data both in transit and at rest? □ Yes □ No

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: ______________________________

Contact information: ________________________________

6. Please provide any additional information that you desire.