NEW HAMPSHIRE STUDENT DATA PRIVACY AGREEMENT VERSION (2019)

Franklin School District

and

iCivics, Inc.

November 17, 2021

This New Hampshire Student Data Privacy Agreement (this "**Agreement**" or this "**DPA**") is entered into by and between Franklin School District (hereinafter referred to as the "**LEA**") and iCivics, Inc. (hereinafter referred to as the "**Provider**") on November 17, 2021. The LEA and the Provider may each be referred to as a "Party" and collectively as the "Parties." The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the LEA with certain digital educational services (the "**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 in New Hampshire the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA; and

WHEREAS, in order to provide the Services described in Article 1 and Exhibit A, the Provider may receive and the LEA may provide data that may be covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("**COPPA**"), 15 U.S.C. 6501-6506, 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., and 34 C.F.R. Part 300; and

WHEREAS, the data transferred from the LEA may also be subject to several New Hampshire student privacy laws, including RSA 189:1-e and 189:65-69; RSA 186, NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of applicable privacy laws, including those referred to above (as applicable), and to establish certain 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 (as defined in Exhibit "C") transmitted to the Provider from the LEA pursuant to Exhibit "A", including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, SOPIPA, RSA 189:1-e and 189:65 through 69, RSA 186-C, NH Admin. Code Ed. 300, NH Admin. Code Ed. 1100 and other applicable New Hampshire state laws, all as may be amended from time to time, as applicable. In performing the Services, to the extent Student Data are transmitted to the Provider from the LEA, the Provider shall be considered a School Official with a legitimate educational interest. The Provider shall be under the direct control and supervision of the LEA with respect to the use of Student Data shared by the LEA with the Provider as set forth in this DPA.

2. **Nature of Services Provided**. The Provider has agreed to provide the digital educational services described in Exhibit "A".

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

4. **DPA Definitions**. The definitions of terms used in this DPA are 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 any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, as applicable, in performing the Services, the Provider shall be considered a School Official under the control and direction of the LEA as it pertains to the use of Student Data transmitted to the Provider from the LEA as set forth in this DPA. The Provider will cooperate and provide Student Data within ten (10) days at the LEA's request.

2. **Parent Access**. The LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records and correct erroneous information, consistent with the functionality of services. The Provider shall cooperate and respond within ten (10) days to the LEA's request for personally identifiable information 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, which will follow the necessary and proper procedures regarding the requested information.

3. **Third Party Request**. Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact the Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request such Student Data directly from the LEA and shall cooperate with the LEA to collect the required information, as permitted under applicable laws. The Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. Except as permitted under this DPA or required under applicable laws, the Provider will not use, disclose, compile, transfer, sell the Student 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 and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of the Provider's services.

4. **No Unauthorized Use**. The Provider shall not use Student Data for any purpose other than as explicitly specified in this DPA or as otherwise required under applicable laws.

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

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws**. The LEA shall provide data for the purposes of this DPA in compliance with the FERPA, PPRA, IDEA, RSA 189:1-e and 189:65 through 69, RSA 186-C, NH Admin. Code Ed. 300, NH Admin. Code Ed. 1100 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**. The 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**. The LEA shall notify the Provider promptly of any known or suspected unauthorized access to the Student Data. The LEA will assist the Provider in any efforts by the Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all New Hampshire and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, RSA 189:1-e and 189:65 through 69, RSA 186-C, NH Admin. Code Ed. 300, NH Admin. Code Ed. 1100 and all other applicable New Hampshire privacy statutes and regulations, as applicable.

2. **Authorized Use**. Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA, as authorized under the applicable statutes referred to in subsection (1) above or as otherwise required under applicable laws. Notwithstanding the foregoing, the Provider may use Student Data in connection with the operation and improvement of the Services or as otherwise required under applicable laws. The Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, there is a court order or lawfully issued subpoena for the information or as otherwise permitted under this DPA, or required under applicable laws.

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

4. **No Disclosure**. De-identified information, as defined in Exhibit "C", may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). The Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written consent has been received from the LEA, in each case other than (i) any such transfers to Subprocessors pursuant to this DPA and (ii) any publications of de-identified and aggregated Student Data that do not name the LEA directly or indirectly (including publications of summary statistics or other information). The Provider shall not copy, reproduce or transmit any Student Data obtained under this DPA and/or any portion thereof, except as necessary to fulfill this DPA or as otherwise required under applicable laws. Prior to publishing any document that presents de-identified Student Data and names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which such de-identified Student Data is presented.

5. **Disposition of Data**. The Provider shall dispose of all personally identifiable information obtained under this DPA within sixty (60) days of (i) the LEA's written request, (ii) the Provider's determination that it is no longer needed for the purpose for which it was obtained or (iii) the date of termination of this DPA, whichever is earliest. Nothing in this DPA authorizes the Provider to maintain Student Data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying or deleting the personal information in those records to make it unreadable or indecipherable. Upon the LEA's reasonable written request, the Provider will confirm that such Student Data has been disposed of. The duty to dispose of Student Data shall not extend to data that has been de-identified. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as Exhibit "D".

6. **Advertising Prohibition**. The Provider is prohibited from leasing, renting, using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by the Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Services to the LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Services to the LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain data security measures, consistent with industry standards and practices, designed to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of the Provider are set forth below. These measures shall include, but are not limited to:

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

b. **Destruction of Data**. The Provider shall dispose of all Personally Identifiable Information contained in Student Data obtained under this DPA upon the LEA's written request or when the Provider determines it is no longer needed for the purpose for which it was obtained. Nothing in this DPA authorizes the Provider to maintain personally identifiable information contained in Student Data beyond the time period reasonably needed to complete the disposition.

c. **Security Protocols**. Both Parties agree to maintain security protocols consistent with industry practices in the transfer or transmission of Student Data, including those designed to ensure that Student Data may only be viewed or accessed by parties legally allowed to do so. The Provider shall maintain all Student Data obtained pursuant to this DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to this DPA, except as necessary to fulfill the purpose of data requests by the LEA, as set forth in this DPA or as otherwise required under applicable laws. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access Student Data.

d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or have access to the Student Data. Further, the Provider shall provide the LEA with contact information of an employee who the LEA may contact if there are any security concerns or questions with respect to the Student Data.

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

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

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

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

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

j. **Audits**. At least five (5) business days following receipt of a reasonable written request from the LEA, and at the LEA's sole cost and expense, at most once a year, except in the case of a verified material data security breach, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student 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 such audit or investigation of the Provider and/or delivery of Services to students and/or the LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and the LEA's Student Data and all records reasonably pertaining to the LEA and delivery of Services to the LEA.

k. **New Hampshire Specific Data Security Requirements**. The Provider agrees to the privacy and security standards from "the Minimum Standards for Privacy and Security of Student and Employee Data" from the New Hampshire Department of Education as set forth in the "iCivics compliance notes" column of the table set forth on Exhibit "F." The LEA hereby acknowledges and agrees that the Provider's performance of the measures in the "iCivics compliance notes" column of the table set forth on Exhibit "F" constitutes full performance of the Provider's obligations under this Article V, Section 1(k) and Exhibit "F."

2. **<u>Data Breach</u>**. In the event that Student Data is accessed or obtained by an unauthorized individual, the Provider shall provide notification to the LEA within thirty (30) days of the Provider's knowledge of such incident. The Provider shall follow the following process:

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 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.

iv. 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.

v. A general description of the breach 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 breach, if any.

c. At the LEA's reasonable discretion, the security breach notification may also include any of the following:

i. Information about what the Provider has done to protect individuals whose information has been breached.

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

d. The Provider agrees to adhere to all applicable requirements in the New Hampshire Data Breach law and in federal law with respect to a data breach related to the Student Data, including, when required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. The Provider further acknowledges and agrees to have a written incident response plan that is consistent with industry standards and applicable federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof and agrees to provide the LEA, upon written request, with a copy of said written incident response plan.

f. Solely as required under applicable laws, and at the reasonable written request and with the assistance of the LEA, the Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA until the end of the 2021-2022 school year.

2. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.

Either Party may terminate this DPA and any service agreement or contract between the Parties if either Party breaches any terms of this DPA.

3. **Effect of Termination**. If this DPA is terminated, the Provider shall dispose of all of the LEA's Student Data pursuant to this DPA. The duty to dispose of Student Data shall not extend to data that has been de-identified.

4. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the applicable legal privacy protections, including those found in FERPA, IDEA, COPPA, PPRA, RSA 189:1-e and 189:65-69, RSA 186, NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100, as applicable. In the event there is conflict between the terms of this 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	Sue Meehan
Title	Chief Operating and Financial Officer
Address	1035 Cambridge Street, Suite 2B
Telephone	617-356-8311 x102
Email	sue.meehan@icivics.org

The designated representative for the LEA for this Agreement is:

Robyn Dunlap, IT Director
rdunlap@sau18.org || 603-671-1255 x2
Franklin School District SAU#18
119 Central Street, Franklin, NH 03235

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

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 OF NEW HAMPSHIRE, 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 MERRIMACK COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority**. The Provider represents that it is authorized to bind to the terms of this Agreement, 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, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.

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

11. **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 DPA 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).

ARTICLE VII:ARTICLE VII- GENERAL OFFER OF TERMS

The Provider and any school district that is not a party to this DPA may, by signing the attached Form of General Offer of Privacy Terms (the "**General Offer**," attached hereto as Exhibit "E"), be bound by the terms of this DPA.

[*Signature Page Follows*]

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

FRANKLIN SCHOOL DISTRICT

By: Robyn Dunlap Date: 11/17/2021

Printed Name: Robyn Dunlap Title/Position: IT Director

ICIVICS, INC.

DocuSigned by:
Sue Meehan
2E46EB4810684AD...

By: Date: November 17, 2021

Printed Name: Sue Meehan Title/Position: COO/CFO

EXHIBIT "A"

DESCRIPTION OF SERVICES

iCivics' educational online games and lesson plans to promote civics education and encourage students to become active citizens.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	x
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	x
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	Student scores and responses to iCivics' online games
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
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	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
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	x
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	x
	Student app username	x
	Student app passwords	x
Student Name	First and/or Last	x
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	x
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	x
	Other student work data - Please specify:	
Transcript	Student course grades	
	Student course data	

Category of Data	Elements	Check if used by your system
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if used by your system
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

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 student records 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. 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, 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 Student Data and metadata, obtained by reason of the use of the Provider's software, website, service, or app, including mobile apps, whether gathered by the Provider or provided by the LEA or its users, students, 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
Political Affiliations
Text Messages
Student Identifiers
Photos
Videos
Grade
Place of birth

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

Unique pupil identifier
Credit card account number, insurance account number, and financial services account number
Name of the student's parents or other family members

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.

Personally Identifiable Information in the Student's Educational Record

Personally Identifiable Information in the Student's Email

Provider: For purposes of this DPA, the term "Provider" has the meaning given to such term in the recitals of this DPA.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including 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 any information that directly relates to a pupil that is maintained by the LEA and provided to the Provider.

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.

Student Data: Student Data includes any data provided by the LEA or its users, students, or students' parents/guardians, that is descriptive of the student, including 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 or geolocation information. 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 the Provider's Services.

Subscribing LEA: An LEA that was not party to this 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 the LEA or the Provider, who the Provider uses for data collection, analytics, storage, or other services, including to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

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

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Franklin School District directs iCivics, Inc. (the "**Provider**") to dispose of data obtained by the Provider pursuant to the terms of the DPA between the LEA and the 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.

3. Signature

____
(Authorized Representative of the LEA)

____
Date

4. Verification of Disposition of Data

________________________________ __________
Authorized Representative of Company Date

EXHIBIT "F"

NEW HAMPSHIRE DATA PRIVACY ATTESTATION

The following table represents an attestation of the measures iCivics takes with respect to the subject matter of each of the following 23 New Hampshire data privacy and security standards from "the Minimum Standards for Privacy and Security of Student and Employee Data" from the New Hampshire Department of Education set forth below.

Summary of iCivics Platform: iCivics.org is hosted on Amazon Web Services and the Drupal platform.

Item	Contract language	iCivics compliance notes
1	Limit system access to the types of transactions and functions that authorized users, such as students, parents, and the LEA, are permitted to execute;	iCivics uses Drupal access control, with roles and permissions set out by Drupal's system of managing access based on users' roles.
2	Limit unsuccessful logon attempts;	Unsuccessful logon limits are set high enough to prevent user error but low enough to impede brute-force attacks admin accounts as well
3	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;	We are using AWS key management, SSH for administration. We use SSL for user interactions combined with strict transport security (STS).
4	Authorize wireless access prior to allowing such connections;	AWS Security Groups allows only whitelisted ip's to ssh to our servers.
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;	AWS Cloudtrail logs are enabled. These provide logs for monitoring, analysis, and investigation of suspicious 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;	CMS actions are tracked with individual users and timestamps. AWS logs provide additional traceability.
7	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;	We use the AWS management console to manage our frontend servers and our database. We maintain replicated systems to serve as development and staging environments throughout the development life cycle. Builds are promoted and deployed using AWS CodeDeploy.
8	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;	Non-public servers are restricted. Nonessential services and applications are shut down when no longer needed.
9	Enforce a minimum password complexity and change of characters when new passwords are created;	We have a minimum password complexity requirement that's enforced for educators, students, and administrators.

10	Perform maintenance on organizational systems;	We have scheduled maintenance for RDS and auto-patching for ec2 instances.
11	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;	All deployments as well as system security patches and periodic maintenance are performed by our release engineer and overseen by our technology director.
12	Ensure equipment removed for off-site maintenance is sanitized of any Student Data in accordance with NIST SP 800-88 Revision 1; 7, 8	Student Data is only approved for storage within servers maintained in the iCivics AWS cloud environment. Student Data is strictly prohibited from being copied. Any equipment removed from the cloud environment is sanitized of any Student Data in accordance with NIST SP 800-88 Revision 1; 7, 8.
13	Protect (i.e., physically control and securely store) system media containing Student Data, both paper and digital;	iCivics maintains Student Data pursuant to applicable laws and regulations in a secure computer environment and does not copy, reproduce, or transmit Student Data, except to perform necessary work.
14	Sanitize or destroy system media containing Student Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse	Student Data must be sanitized in accordance with NIST SP 800-88 Revisions, 1,7,8. Student Data is removed when a user submits a request for data removal or retrieval. iCivics destroys or deletes all personally identifiable information contained in the environment upon written request or when the organization determines it is no longer needed for the purpose for which it was obtained.
15	Control access to media containing Student Data and maintain accountability for media during transport outside of controlled areas	iCivics maintains Student Data pursuant to applicable laws and regulations in a secure computer environment and not copy, reproduce, or transmit Student Data, except to perform necessary work. Sensitive, personally identifiable information is kept secure within internal organizational control and prohibited from being shared with any external parties (other than as explicitly authorized, as permitted under applicable laws or regulations, or to operate and improve products or services).
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	We run a security scan twice per year and remediate any deficiencies that are discovered.

	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	We protect communications and transmissions by using security groups and ensuring access is limited by these groups.
18	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception)	All communication is denied by default and only permitted by exception. We use AWS tools to monitor communications traffic.
19	Protect the confidentiality of Student Data at rest;	Sensitive information must be encrypted in transit and at rest. Locations containing sensitive information at rest (such as production databases) are required to utilize encryption technology. Sensitive information being shared inside or outside of the network shall only be shared via secure mechanisms, such as SFTP, or via encrypted email or attachment.
20	Identify, report, and correct system flaws in a timely manner	We do this via patches when available. We use Jira as an issue tracking tool to track any system flaws or patches. Reports of these issues go to iCivics management
21	Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems	We partner with a firm StratusIT who manages all of our systems and provides antivirus and antimalware.
22	Monitor system security alerts and advisories and take action in response; and	We continuously monitor security advisories about vulnerabilities and patch systems as soon as the patches become available.
23	Update malicious code protection mechanisms when new releases are available	As 21, we monitor and patch systems as patches become available.

NH_iCivics_FranklinNH_VendorSigned

Final Audit Report 2021-11-17

Created:	2021-11-17
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAk8QtEPJ0PhbY2mYmOi2EPM8pHbv7dkuo

"NH_iCivics_FranklinNH_VendorSigned" History

Document created by Ramah Hawley (rhawley@tec-coop.org)

2021-11-17 - 3:51:29 PM GMT- IP address: 74.102.102.44

Document emailed to Robyn Dunlap (rdunlap@sau18.org) for signature

2021-11-17 - 3:51:56 PM GMT

Email viewed by Robyn Dunlap (rdunlap@sau18.org)

2021-11-17 - 3:53:15 PM GMT- IP address: 18.206.199.142

Document e-signed by Robyn Dunlap (rdunlap@sau18.org)

Signature Date: 2021-11-17 - 4:02:07 PM GMT - Time Source: server- IP address: 66.211.132.114

✓ Agreement completed.

2021-11-17 - 4:02:07 PM GMT