DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

Bill of Rights for Data Privacy and Security

AND

Vendor Information Regarding Data Privacy and Security

This Data Sharing and Confidentiality Agreement (the "**Agreement**" or this "**Agreement**") is made and entered into by and between iCivics, Inc. (the "**Vendor**") and Shenendehowa Central School District (also referred to as "**School District**").

WHEREAS, Vendor acknowledges that it may receive and/or come into contact with certain personally identifiable information, as defined by New York Education Law Section 2-d, from records maintained by School District that directly relate to a student(s) ("**Student Data**"), teacher(s) or principal(s) that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "**New York Education Law Section 2-d**" or "**Section 2-d**") in connection with providing certain products or services to School District (such products or services, the "**Services**" and together with Student Data, "**Protected Data**"); and

WHEREAS, both School District and Vendor are desirous of fulfilling their respective obligations under New York Education Law Section 2-d.

NOW THEREFORE, in consideration of the mutual promises and covenants contained in this Agreement, the parties hereto mutually agree as follows:

1. **Confidentiality**

   a. Vendor, its employees, and/or agents agree that Protected Data may include confidential information.

   b. Vendor further agrees to maintain the confidentiality of the Protected Data it receives in accordance with applicable federal and state law and School District's data security and privacy policy, as provided to Vendor in writing.

2. **Data Protections and Internal Controls**

   a. Vendor understands and acknowledges that it shall have in place protections and internal controls to ensure that Student Data is safeguarded in accordance with applicable laws and regulations, and understands and agrees that it is responsible for complying with applicable state data security and privacy standards for the Student Data from education records, and it shall:

      1. Limit internal access to Student Data to those individuals that need to use Student Data in connection with providing the Services; and

      2. Not use the Student Data for any other purpose than (i) those explicitly authorized in the Agreement or the Vendor's privacy policy, (ii) as permitted under applicable laws or (iii) to operate and improve the Vendor's products or services; and

3. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of the Student Data in its custody; and

4. To use encryption technology to protect the Student Data in its custody while in motion or at rest.

3. **Data Security and Privacy Plan**

a. Vendor agrees to have a data security and privacy plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from School District, which shall:

1. Outline how all applicable state, federal and local data security and privacy contract requirements will be implemented over the life of the Agreement consistent with School District's policy on data security and privacy, as provided to Vendor in writing.

2. Outline specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from School District.

3. Outline the training requirement established by the Vendor for all employees who will have access to the Protected Data.

4. **Notice of Breach and Unauthorized Release**

a. In the event of an unauthorized release of Student Data, the Vendor shall:

1. Notify School District within a reasonable time, but no more than seven (7) calendar days, after Vendor has discovered or been informed of the unauthorized release.

2. Advise School District as to the nature of the unauthorized release and steps Vendor has taken to minimize said unauthorized release.

b. In the case of required notification to a parent or eligible student of an unauthorized release of Student Data, the Vendor shall reimburse School District for the full costs of such notification.

c. Vendor will cooperate with School District and provide certain information to School District about the incident, including but not limited to:

1. The description of the incident;

2. The date of the incident;

3. The date Vendor discovered or was informed of the incident;

4. A description of the types of Student Data involved;

5. An estimate of the number of records affected;

6. The school affected;

7. What the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Student Data; and

8. The contact information for Vendor representatives who can assist affected individuals that may have additional questions.

d. Vendor acknowledges that upon initial notification from Vendor, School District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("**CPO**"). Vendor agrees not to provide this notification to the CPO directly unless requested by School District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by School District, Vendor will promptly inform School District of the same.

5. Vendor Information

Vendor understands that as part of School District's obligations under New York Education Law Section 2-d, Vendor is responsible for providing School District with certain Vendor information (see Annex A (Vendor Information for Data Privacy and Security)) to include:

a. Exclusive purposes for which the Student Data will be used;

b. How Vendor will ensure that subcontractors, persons or entities that Vendor will share the Student Data with, if any, will abide by data protection and security requirements;

c. That the Student Data will be returned or destroyed upon expiration of the Agreement, in accordance with the Vendor's standard practices;

d. If and how a parent, student, or eligible teacher may challenge the accuracy of the Protected Data that is collected; and

e. Where the Student Data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

6. Termination or Expiration of Contract and/or Agreement

a. Upon termination of the Agreement, Vendor shall return or destroy the Protected Data obtained in connection with the Services.

b. Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, or copies, summaries or extracts of the Protected Data, on any storage medium whatsoever.

7. **Limitation of Liability**

a. IN NO EVENT SHALL EITHER PARTY BE LIABLE WITH RESPECT TO THIS AGREEMENT OR ANY BREACH THEREOF FOR ANY AMOUNT IN EXCESS OF TEN THOUSAND US DOLLARS ($10,000). IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES WHATSOEVER WHICH IN ANY WAY ARISE OUT OF, RELATE TO, OR ARE A CONSEQUENCE OF, ITS PERFORMANCE OR NONPERFORMANCE UNDER THIS AGREEMENT, WHETHER SUCH ACTION IS BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY) OR OTHERWISE, EVEN IF AN AUTHORIZED REPRESENTATIVE OF SUCH PARTY IS ADVISED OF THE POSSIBILITY OR LIKELIHOOD OF THE SAME. SPECIAL DAMAGES UNDER THIS AGREEMENT INCLUDE, BUT ARE NOT LIMITED TO, LOSS OF PROFITS, BUSINESS INTERRUPTIONS AND CLAIMS OF CUSTOMERS. NOTWITHSTANDING THE FOREGOING, IN THE EVENT A BREACH OR UNAUTHORIZED RELEASE OF STUDENT DATA IS ATTRIBUTED TO VENDOR, VENDOR SHALL PAY FOR OR PROMPTLY REIMBURSE SCHOOL DISTRICT FOR THE FULL COST OF REQUIRED NOTIFICATIONS IN CONNECTION THEREWITH.

8. **Governing Law, Venue and Jurisdiction**

a. This Agreement shall be governed by and construed in accordance with the laws of the state of New York, 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 New York County for any dispute arising out of or relating to this Agreement.

9. **Entire Agreement**

a. This Agreement constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties. This Agreement may be amended only with the signed written consent of both parties.

DocuSigned by:
Sue Meehan
2E46EB4810684AD...

1/5/2022

Authorized Vendor Signature

Date

Rebecca Cairns (DPO)

Authorized School District Signature

12/20/21

Date

ANNEX A

VENDOR INFORMATION REGARDING DATA PRIVACY AND SECURITY

Vendor: iCivics, Inc. Product: Civics learning platform

Collects: ☒ Student Data ☐ Teacher or Principal Data ☐ Does not collect either

Educational agencies including Shenendehowa Central School District are required to *post information about third-party contracts on the agency's website* with the Parents Bill of Rights. To that end, please complete the table below with information relevant to NYS Education Law 2-d and Part 121.3 of the Commissioner's Regulations. Note that this applies to all software applications and to mobile applications ("apps").

Part 1: Exclusive Purposes for Data Use
The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor: To provide, improve and operate its products and services; as permitted under applicable laws and regulations; and as explicitly authorized.
Part 2: Subcontractor Oversight Details – Select the appropriate option below.
☐ This contract has no subcontractors. ☒ This contract has subcontractors. As such, the third-party contractor will take the following steps to ensure that any subcontractors, assignees, or other agents who see, or receive, Student Data are contractually required to obey the same data protection and security requirements that the third-party contractor is required to obey under state and federal law: Subcontractors with access to student data must sign confidentiality agreements or be subject to other appropriate confidentiality restrictions before accessing the data.
Part 3: Contract Lifecycle Practices
The contract expires at the end of the 2021-2022 school year, unless renewed or automatically extended for a term pursuant to the agreement. When the contract expires, Student Data will be deleted by the contractor, via shredding, returning of data, mass deletion, and upon request, may be exported for use by Shenendehowa Central School District before deletion.
Part 4: Student Educational Records / Improper Disclosure
A. For information on FERPA (Family Educational Rights and Privacy Act), which is the federal law that protects the privacy of student education records, visit the U.S. Department of Education FERPA website. B. A complaint or report of improper disclosure may be completed by submitting the Improper Disclosure Report form.
Part 5: Security Practices
A. Student Data provided to the contractor will be stored: (include *where* and *how*) Student data is in an encrypted database hosted by Amazon Web Services (AWS). B. The security protections taken to ensure Student Data will be protected that align with the NIST Cybersecurity Framework and industry best practices include: Encryption utilized for all traffic over public, untrusted networks. Locations (e.g., production databases) containing student data required to utilize encryption. Sensitive data being shared outside of the network shall only be shared via secure mechanisms, such as SFTP or encrypted email.
Part 6: Encryption Practices
☒ By checking this box, contractor certifies that encryption of Student Data is applied in accordance with NYS Education Law Section 2-d 5(f)(5).

Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, place of birth, social security number, biometric record & mother's maiden name, which when linked to or combined with other information that, alone or in combination, is linked or linkable to a specific student and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or any information requested by a person if the educational agency or institution reasonably believes that person knows the identity of the student to whom the education record relate

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the Shenendehowa Central School District, Director of Policy & Community Development/Data Protection Officer, 5 Chelsea Place, Clifton Park, NY 12065. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.