Vendor Specific

Standard Student Data Privacy Agreement

IL-NDPA v1.0a

School District or LEA

Park Ridge-Niles Community Consolidated School District 64

and

Provider

iCivics, Inc.

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Park Ridge-Niles Community Consolidated School District 64, located at 164 S. Prospect Ave, Park Ridge IL 60068 (the "**Local Education Agency**" or "**LEA**") and iCivics, Inc., located at 1035 Cambridge Street, Suite 21B, Cambridge, MA 02141 (the "**Provider**").

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

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

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

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

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions**. *Check if Required*
   - ☑ If checked, the Supplemental State Terms attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.
   - ☐ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H"**. (**Optional**)
   - ☑ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms.

3. In the event of a conflict between the Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Provider terms of service or privacy policy, the terms of this DPA shall control.

4. This DPA shall stay in effect for three years. **Exhibit "E"**, and each executed version thereof, will expire automatically upon the termination or expiration of the original DPA.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Mary Jane Warden_____ Title: Privacy Officer_____

Address: 164 S. Prospect Ave, Park Ridge IL 60068_____

Phone: 847 318 4300_____ Email: privacy@d64.org_____

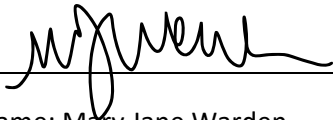The designated representative for the Provider for this DPA is:

Name: Sue Meehan_____ Title: COO/CFO_____

Address: 1035 Cambridge Street, Suite 21B_____

Phone: 617-356-8311 x102_____ Email: legal@icivics.org_____

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

LEA:

By: _____ Date: ___9/21/2021_____

Printed Name: Mary Jane Warden_____ Title/Position: Director of Technology

Provider: iCivics, Inc.

By: _____ Date: _____

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

9/17/2021

<u>**STANDARD CLAUSES**</u>
Version 1.0

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, including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, 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 its use of Student Data as set forth in this DPA.

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

3. **DPA Definitions**. The definitions of terms used but not otherwise defined 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 any other writing, including, but not limited to the Provider's terms of service, privacy policies, etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to this DPA is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per this DPA, shall remain the exclusive property of the LEA. For the purposes of FERPA, 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 as set forth in this DPA.

2. **Parent Access**. To the extent required by law, the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data and correct erroneous information, consistent with the functionality of the Services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, which will follow the necessary and proper procedures regarding the requested information.

3. **Law Enforcement Requests**. Should law enforcement or other government entities ("**Requesting Party(ies)**") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

4. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to this DPA, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access to the Student 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 with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

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

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under this DPA. 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**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including personally identifiable information contained in the Student Data, other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to De-Identified Data, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the

Provider pursuant to this DPA, or as otherwise set forth under this DPA or required by applicable law. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and applicable law and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's ability to use De-Identified Data shall survive termination of this DPA or any request by LEA to dispose of, return or destroy Student Data. Except for Subprocessors, Provider agrees 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 notice has been given to the LEA who has provided prior written consent for such transfer, in each case other than 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). 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 such publication and the manner in which such De-Identified Student Data is presented.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or transfer to the LEA Student Data obtained under this DPA, within sixty (60) days of the date of said request. Upon termination of this DPA, if no written request from the LEA is received, Provider shall destroy all Student Data. The duty to dispose of, return or destroy Student Data shall not extend to Student 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"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

ARTICLE V: DATA PROVISIONS

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

2. **Audits.** No more than once a year, or following a material unauthorized access to Student Data in the Provider's possession, upon receipt of a reasonable written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, and at the LEA's sole cost and expense, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it

pertains to the delivery of services to the LEA during reasonable business hours. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any such audit of the Provider and/or delivery of Services to LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records reasonably pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of this DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. Provider shall provide, in the Standard Schedule to this DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within five (5) business days of Provider's confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

    (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

        i.   The name and contact information of the reporting LEA subject to this section.
        ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
        iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
        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; and
        v.   A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

    (2) Provider agrees to adhere to all applicable federal and state legal requirements 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.

    (3) 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, including personally identifiable information and agrees to provide LEA, upon written request, with a summary of said written incident response plan.

(4)   LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5)   In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent reasonably necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider and any Subscribing LEA that is not a party to this DPA 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 DPA. The General Offer is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1.   **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent. Either party may terminate this DPA if the other party breaches any terms of this DPA.

2.   **Effect of Termination**. If this DPA is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3.   **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the applicable privacy protections, including those found in FERPA, as applicable, and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of this DPA and Provider's terms of service or privacy policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control.

4.   **Entire Agreement**. This DPA, together with Provider's terms of service and privacy policy, 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.

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

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

7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within this 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.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

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

10. **Limitation of Liability**. iCivics is a nonprofit organization with limited resources, which provides products and services to its users at no cost. EXCEPT IN THE EVENT OF A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, IN NO EVENT SHALL EITHER PARTY BE LIABLE (i) WITH RESPECT TO THIS DPA OR ANY BREACH THEREOF FOR ANY AMOUNT IN EXCESS OF TEN THOUSAND US DOLLARS ($10,000) AND (ii) 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 DPA, 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 DPA INCLUDE, BUT ARE NOT LIMITED TO, LOSS OF PROFITS, BUSINESS INTERRUPTIONS AND CLAIMS OF CUSTOMERS.

EXHIBIT "A"
DESCRIPTION OF SERVICES

https://www.icivics.org/

A platform to engage students in meaningful civic learning. They provide teachers well-written, inventive, and free resources that enhance their practice and inspire their classrooms.

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.	✓
	Other application technology meta data-Please specify:	☐
Application Use Statistics	Meta data on user interaction with application	✓
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 captured (emails, blog entries)	☐
Conduct	Conduct or behavioral data	☐
Demographics	Date of Birth	☐
	Place of Birth	☐
	Gender	☐
	Ethnicity or race	☐
	Language information (native, or primary language spoken by student)	☐
	Other demographic information-Please specify:	☐
		☐
Enrollment	Student school enrollment	☐
	Student grade level	☐
	Homeroom	☐
	Guidance counselor	☐
	Specific curriculum programs	☐
	Year of graduation	☐
	Other enrollment information-Please specify:	☐
Parent/Guardian Contact	Address	☐

Category of Data	Elements	Check if Used by Your System
Information	Email	☐
Category of Data	**Elements**	**Check if Used by Your System**
	Phone	☐
Parent/Guardian ID	Parent ID number (created to link parents to students)	☐
Parent/Guardian Name	First and/or Last	☐
Schedule	Student scheduled courses	☐
	Teacher names	☐
Special Indicator	English language learner information	☐
	Low income status	☐
	Medical alerts/ health data	☐
	Student disability information	☐
	Specialized education services (IEP or 504)	☐
	Living situations (homeless/foster care)	☐
	Other indicator information-Please specify:	☐
Student Contact Information	Address	☐
	Email	✓
	Phone	☐
Student Identifiers	Local (School district) ID number	☐
	State ID number	☐
	Provider/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	✓
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	✓
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	☐
Student Survey Responses	Student responses to surveys or questionnaires	☐
Student work	Student generated content; writing, pictures, etc.	✓
	Other student work data -Please specify:	☐

Category of Data	Elements	Check if Used by Your System
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	☐
	Student bus card ID number	☐
	Other transportation data - Please specify:	☐

Category of Data	Elements	Check if Used by Your System
Other	Please list each additional data element used, stored, or collected by your application:	☐
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

EXHIBIT "C"
DEFINITIONS

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

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation. Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes.

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

Student Generated Content: The term "Student-Generated Content" means materials or content created by a student in the services including essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

Student Data: Student Data means any data, whether gathered by Provider from, or provided by, 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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide personal information about a specific student. Student Data includes "Personally Identifiable Information (PII)" as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for

the purposes of applicable federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's Services.

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

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

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

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

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

Provider to dispose of Student Data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the disposition are set forth below:

1. Extent of Disposition

   ☐ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this directive.

   [   ]

   ☐ 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:

   [   ]

3. Signature

   _____   _____
   Authorized Representative of LEA   Date

4. Verification of Disposition of Data

   _____   _____
   Authorized Representative of Provider   Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

iCivics, Inc. ("**Provider**") offers the same privacy protections found in that certain Student Data Privacy Agreement ("**DPA**") between it and Park Ridge-Niles Community Consolidated School District 64 ("Originating LEA") which is dated September 21, 2021, to any other local education agency in the state of Illinois ("**Subscribing LEA**") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to any other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the DPA; or (3) the earlier of three (3) years after the date of Provider's signature to this General Offer and the expiration or termination of the DPA. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: legal@icivics.org.

PROVIDER: iCivics, Inc.

By: _Sue Meehan_   Date: 9/17/2021

2E46EB4810684AD...

Printed Name: Sue Meehan_____   Title/Position: COO/CFO_____

2. Subscribing LEA

A Subscribing LEA, by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of the DPA for the term of the DPA.

Subscribing LEA:

By: _____   Date: _____

Printed Name: _____   Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Intentionally omitted.

EXHIBIT "G" – Supplemental SDPC (Student Data Privacy
Consortium) State Terms for Illinois
Version IL-NDPAv1.0a (Revised March 15, 2021)

This **Exhibit "G"**, Supplemental SDPC State Terms for Illinois ("**Supplemental State Terms**"), effective simultaneously with the attached Student Data Privacy Agreement ("**DPA**") by and between Park Ridge-Niles Community Consolidated School District 64 (the "**Local Education Agency**" or "**LEA**") and iCivics, Inc. (the "**Provider**"), is incorporated in the attached DPA and supplements the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Compliance with Illinois Privacy Laws**. In performing their respective obligations under the Agreement, the LEA and the Provider shall comply with all applicable Illinois laws and regulations pertaining to student data privacy, confidentiality, and maintenance, including but not limited to the Illinois School Student Records Act ("**ISSRA**"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("**MHDDCA**"), 740 ILCS 110/, Student Online Personal Protection Act ("**SOPPA**"), 105 ILCS 85/, Identity Protection Act ("**IPA**"), 5 ILCS 179/, and Personal Information Protection Act ("**PIPA**"), 815 ILCS 530/, and Local Records Act ("**LRA**"), 50 ILCS 205/, as applicable.

2. **Definition of "Student Data."** In addition to the definition set forth in **Exhibit "C"**, Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)), (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA.

3. **School Official Designation.** Pursuant to Article I, Paragraph 1 of the DPA Standard Clauses, and in accordance with FERPA, ISSRA and SOPPA, as applicable, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; and is under the direct control of the LEA with respect to the use and maintenance of Student Data as set forth in the DPA and is using Student Data only for an authorized purpose in accordance with the terms of the DPA and in furtherance of such legitimate educational interest.

4. **Limitations on Re-Disclosure.** The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA or otherwise permitted under the DPA or required by applicable law. Provider will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall redirect the other party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon written request, provide the LEA with a copy of the court order requiring such disclosure.

5. **Notices.** Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.

6. **Parent Right to Access and Challenge Student Data.** The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). The Provider shall respond to any request by the LEA for Student Data in the possession of the Provider when Provider cooperation is required to afford a parent an opportunity to inspect and/or copy the Student Data, no later than 45 days from the date of the request. In the event that a parent contacts the Provider directly to inspect and/or copy Student Data, the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data.

7. **Corrections to Factual Inaccuracies.** In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy.

8. **Security Standards.** The Provider shall implement and maintain commercially reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect Student Data from unauthorized access, destruction, use, modification, or disclosure, including but not limited to the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the Student Data (a "**Security Breach**"). For purposes of the DPA and this **Exhibit "G"**, "Security Breach" does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA, as applicable, and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.

9. **Security Breach Notification**. In addition to the information enumerated in Article V, Section 4(1) of the DPA Standard Clauses, any Security Breach notification provided by the Provider to the LEA shall include:

   a. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and

   b. The email address for the Provider whom parents may contact to inquire about the breach, which email address shall be legal@icivics.org.

10. **Expenses Associated with Security Breach.** iCivics is a nonprofit organization with limited resources, which provides products and services to its users at no cost. In the event of a Security Breach that is attributable to the Provider, the LEA shall be responsible for any and all reasonable costs and expenses that the LEA incurs in investigating and remediating the Security Breach.

11. **Transfer or Deletion of Student Data.** If the Provider determines any of the Student Data is no longer needed for purposes of the DPA, the Provider must delete such unnecessary Student Data or transfer to the LEA such unnecessary Student Data. Except as prohibited by applicable law, the Provider will delete Student Data within the timeframe allocated in Provider's data retention policies if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. The duty to dispose of, return or destroy Student Data shall not extend to Student Data that has been de-identified.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

12. **Public Posting of DPA.** Pursuant to SOPPA, the LEA shall publish on its website a copy of the DPA between the Provider and the LEA, including this **Exhibit "G"**.

13. **Subcontractors**. By no later than five (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data is disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data is disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).

13. **Privacy Policy.** The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

14. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.

15. **Student and Parent Access.** Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.

16. **Data Storage.** Provider shall store all Student Data shared under the DPA within the United States.

17. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.

EXHIBIT "H"
Additional Terms or Modifications
Version 1.0a

LEA and Provider agree to the following additional terms and modifications:

None.