AN ACT TO PROTECT STUDENT PRIVACY WITH RESPECT TO ELECTRONIC DATA ON 1-TO-1 PROGRAM DEVICES

Be it enacted by the {fill in appropriate language for your state}:

Section 1 – Definitions: For the purposes of this Act:

(A) "1-to-1 program" shall mean any program authorized by an educational institution where a technological device is provided to a student by or through an educational institution for overnight or at-home use.

(B) "1-to-1 device" shall mean a technological device provided to a student pursuant to a 1-to-1 program.

(C) "1-to-1 device provider" shall mean a person or entity that provides a 1-to-1 device to a student or educational institution pursuant to a 1-to-1 program, and includes any business or non-profit entities that share a parent, subsidiary, or sister relationship with the entity that provides the 1-to-1 device.

(D) "Aggregate data" shall mean student-related data collected and reported by an educational institution at the group, cohort, or institutional level that contains no personally identifiable student information.

(E) "De-identified" shall mean having removed or obscured any personally identifiable information from personally identifiable student information in a manner that prevents the unintended disclosure of the identity of the student and/or information about the student. Information shall not be considered de-identified if it meets the definition of "personally identifiable student information" in Section 1(J).

(F) "Educational institution" shall mean:

(1) A private, public, or publically funded school, institution, or school district, or any subdivision thereof, that offers participants, students or trainees an organized course of study or training that is academic, trade-oriented, or preparatory for gainful employment, as well as school employees acting under the authority or on behalf of an educational institution; or

(2) A state or local educational agency authorized to direct or control an entity in Section 1(F)(1).

(G) "Elementary school" shall mean the grade levels falling under the definition of "elementary school," as that term is interpreted by state law for purposes of Section 9101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. §7801 *et seq.*).

(H) "Location tracking technology" shall mean any hardware, software, or application that collects and/or reports data that identifies the geophysical location of a technological device.

(I) "Opt-in agreement" shall mean a discrete, verifiable, written or electronically generated agreement by which, subject to the provisions of this Act, a student and/or the student's parent or legal guardian voluntarily grants a school employee or 1-to-1 device provider with limited permission to access and interact with a specifically defined set of personally identifiable student information.

(J) "Personally identifiable student information" shall mean one or more of the following:

(1) A student's name;

(2) The name of a student's parent, legal guardian, or other family member;

(3) The address of a student or student's parent, legal guardian, or other family member;

(4) A photograph, video, or audio recording that contains the student's image or voice;

(5) Indirect identifiers, including but not limited to a student's date of birth, place of birth, mother's maiden name, social security number, student number, biometric record, telephone number, credit card account number, insurance account number, financial services account number, customer number, persistent online identifier, email address, social media address, and other electronic address;

(6) Any aggregate or de-identified student data that, through reasonable effort, is capable of being de-aggregated or reconstructed to the point that individual students can be identified; and

(7) Any student-generated content or data or other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person, who does not have personal knowledge of the relevant circumstances, to identify a specific student with reasonable certainty.

(K) "School employee" shall mean an individual who is employed by an educational institution, compensated through an annual salary, hourly wage, or other form of compensation paid by an educational institution, and whose services for which the compensation is provided are primarily rendered at a physical location which is owned or leased by that educational institution. For purposes of this Act, a school enforcement official shall not be considered a school employee.

(L) "School enforcement official" shall mean any school employee with law enforcement or school security responsibilities, including a school resource officer, school district police officer, contract or private security company employee, security guards or other security personnel, but shall not include any sworn law enforcement officers.

(M) "Student" shall mean any student, participant or trainee, whether full-time or part-time, in an organized course of study at an educational institution.

(N) "Student-generated content or data" shall mean any files, information, or data that is created as a result of a student's interaction with a 1-1 device.

(O) "Sworn law enforcement officer" shall mean any person formally authorized to make arrests while acting within the scope of explicit legal authority.

(P) "Technological device" shall mean any computer, cellular phone, smartphone, digital camera, video camera, audio recording device, or other electronic device that can be used for creating, storing, or transmitting information in the form of electronic data.

Section 2 – 1-to-1 Programs:

(A) Where an educational institution or 1-to-1 device provider provides a student with a technological device pursuant to a 1-to-1 program, no school employee, school enforcement official, or 1-to-1 device provider, or an agent thereof, may access or track such a device or the activity, student-generated content, or data stored or created

Comment [CM1]: *NOTE TO AFFILAITES: This is done so the terminology in consistent if this is combined with other ACLU student data privacy model bills.*

Comment [CM2]: *NOTE TO AFFILIATES: Your state may already have a definition of this term.*

thereupon, or enable any other person or entity to do so, either remotely or in person, except in accordance with the provisions of this Act.

(B) No school employee, school enforcement official, or 1-to-1 device provider, or an agent thereof, may access any student-generated content or data input into, stored upon, or sent or received by a student's 1-to-1 device, including but not limited to its browser, key stroke or location history, nor may such student-generated content or data be analyzed, interacted with, shared, and/or transferred unless:

(1) The student-generated content or data being collected is not personally identifiable student information;

(2) The student-generated content or data is being accessed by or on behalf of school employee who:

(a) Is the student's teacher, or is subject to the student's teacher's supervision and is assisting that teacher in the classroom;

(b) Is receiving or reviewing the student-generated content or data for an educational purpose consistent with the teacher's professional duties; and

(c) Does not use the student-generated content or data, or permit any other person or entity to use the student-generated content or data, for any other purpose.

(3) A school employee or 1-to-1 device provider or an agent thereof has been authorized to access specific personally identifiable student information pursuant to a Section 2(I) opt-in agreement;

(4) A school employee or school enforcement official has a reasonable suspicion that the student has violated or is violating an educational institution policy and that student-generated content or data on the 1-to-1 device contains evidence of the suspected violation, subject to the following limitations:

(a) Prior to searching a student's 1-to-1 device based on reasonable individualized suspicion, the school employee or school enforcement official shall document the reasonable individualized suspicion and notify the student and the student's parent or legal guardian of the suspected

violation and what student-generated content or data will be accessed in searching for evidence of the violation.

(i) An educational institution, school employee, or school enforcement official, subject to any other relevant legal restrictions, may seize a student's 1-to-1 device to prevent data deletion pending notification, provided that:

a. The pre-notification seizure period is no greater than 48 hours; and

b. The 1-to-1 device is stored securely on educational institution property and not accessed during the pre-notification seizure period.

(b) Searches of a student's device based upon a reasonable individualized suspicion that an educational institution policy has been violated shall be strictly limited to finding evidence of the suspected policy violation and shall immediately cease upon finding sufficient evidence of the suspected violation or evidence that such a violation did not occur.

(i) It shall be a violation of this subsection to copy, share, or transfer any student-generated content or data, or any information thereabout, that is unrelated to the specific suspected violation which prompted the search of the 1-to-1 device.

(c) Where a student is suspected of illegal conduct, no search of the 1-to-1 device may occur unless the student's parent or legal guardian have first been notified and a judicial warrant, based on a probable cause standard, has been secured in accordance with Section 2(B)(5), even if the student is also suspected of a related or unrelated violation of educational institution policy.

(5) A school employee or school enforcement official:

(a) Reasonably suspects a student has engaged or is engaging in illegal conduct;

(b) Reasonably suspects student-generated content or data on the 1-to-1 device contains evidence of the suspected illegal conduct;

(c) Has notified the student's parent or legal guardian of the suspicion and the educational institution's interest in having the device searched;

(d) Has requested a sworn law enforcement officer search the 1-to-1 device; and

(e) The sworn law enforcement officer has secured a judicial warrant, based on a probable cause standard, authorizing the officer to search the 1-to-1 device.

(f) Section 2(B)(5) shall apply even if a student is also suspected of a related or unrelated violation of an educational institution policy

(6) Doing so is necessary to update or upgrade device's software, or protect the device from cyber-threats, and access is limited to that purpose;

(7) Doing so is required by law, and access to the data, and the interaction therewith, is limited to fulfilling the legal requirement;

(8) The data is promptly de-identified and aggregated, and the personally identifiable student information is then immediately deleted and destroyed;

(9) Doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose; or

(a) Within 72 hours of accessing a 1-to-1 device's data in response to an imminent threat to life or safety, the school employee, school enforcement official, or sworn law enforcement officer who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution with a written description of the precise threat that prompted the access and what student-generated content or data was accessed.

(10)The student-generated content or data sent from the device is posted on a website or website account that:

(a) Is accessible by the general public;

(b) Was created by the educational institution or a school employee for the purpose of enabling students to share student-generated content or data with the educational institution and/or their teacher(s) and classmates; or

(c) Is accessible by a specific school employee or school enforcement official who was granted permission by the student to view the content.

(C) No school employee, school enforcement official, sworn law enforcement officer, or 1-to-1 device provider, or an agent thereof, may use a student's 1-to-1 device's location tracking technology to track a device's real-time or historical location, unless:

(1) Location tracking is necessary to the educational function of software on the 1-to-1 device, and permission for the specific software to track location data has been granted pursuant to a Section 2(I) opt-in agreement.

(2) Such use is ordered pursuant to a judicial warrant, based on a probable cause standard;

(3) The student to whom the device was provided, or the student's parent or legal guardian, has notified a school employee, school enforcement official, or law enforcement official that the device is missing or stolen; or

(4) Doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose.

(a) Within 72 hours of accessing a 1-to-1 device's location tracking technology is accessed in response to an imminent threat to life or safety, the school employee, school enforcement official, or sworn law enforcement officer who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what student-generated content or data and features were accessed.

(D) No school employee, school enforcement official, or 1-to-1 device provider, or an agent thereof, may activate or access any audio or video receiving, transmitting, or recording functions on a student's 1-to-1 device, unless:

(1) A student initiates a video chat or audio chat with the school employee or 1-to-1 device provider;

(2) The activation and/or access is ordered pursuant to a judicial warrant, based on a probable cause standard.

(3) Doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose.

(a) Within 72 hours of accessing a 1-to-1 device's audio or video receiving, transmitting, and/or recording functions are accessed in response to an imminent threat to life or safety, the school employee, school enforcement official, or sworn law enforcement officer who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what student-generated content or data and features were accessed.

(E) No school employee, school enforcement official, or an agent thereof, may use a 1-to-1 device, or require a student to use a 1-to-1 device in their presence, in order to view or gain access to a student's password protected software, website accounts, or applications, except where:

(1) The school employee is a teacher;

(2) The student is enrolled in and participating in a class taught by the teacher; and

(3) The viewing of the 1-to-1 device relates exclusively to an educational purpose.

(F) No 1-to-1 device provider, or an agent thereof, may use any personally identifiable student information stored on or retrieved from a 1-to-1 device to:

(1) Inform, influence, or direct marketing or advertising efforts directed at a student, a student's parent or legal guardian, or a school employee, except pursuant to a valid opt-in agreement; or

(2) Develop, in full or in part, a student profile for any commercial or other non-educational purpose.

(G) Notwithstanding any other provisions in this Act, no school employee may supervise, direct, or participate in a 1-to-1 program, or access any 1-to-1 device or data thereupon, until she has received adequate training to ensure the school employee's understanding and compliance with the provisions of this Act.

(H) No school employee or 1-to-1 device provider, or an agent thereof, who receives or collects student-generated content or data or personally identifiable student information from a 1-to-1 device may share, sell or otherwise transfer such data to another person or entity except:

(1) To another school employee who has satisfied the requirements of Section 2(G) and is accessing the student-generated content or data or personally identifiable student information in furtherance of the employee's professional duties;

(2) Where a 1-to-1 device provider has been authorized to do so pursuant to a Section 2(I) opt-in agreement; or

(3) In the case of a 1-to-1 device provider, where such information is sold as part of a sale or merger of the entirety of the 1-to-1 device provider's business.

(a) Any entity that purchases student-generated content or data or personally identifiable student information pursuant to Section 2(H)(3) shall be subject to the same restrictions and obligations under this Act as the 1-to-1 device provider from which the student-generated content or data or personally identifiable student information was obtained.

(I) Opt-In Agreements

(1) For purposes of this Act, an opt-in agreement shall only be valid if it identifies, with specificity:

(a) The precise subset of student-generated content or data or personally identifiable student information on the 1-to-1 device to which the authority to access, analyze, and interact is being granted;

(b) The name of the school employee(s) or 1-to-1 device provider to whom the authority to access, analyze and interact with the student-generated

content or data or personally identifiable student information on the 1-to-1 device is being granted;

(c) The educational purpose(s) for which the school employee(s) or 1-to-1 device provider is being granted the authority to access, analyze and interact with the student-generated content or data or personally identifiable student information on the 1-to-1 device; and

(d) The individual student to whom the opt-in agreement applies.

(2) An opt-in agreement shall only be valid if it has been signed or otherwise affirmatively agreed to in a verifiable format by:

(a) The student's parent or guardian, if the student is in elementary school;

(b) The student and the student's parent or legal guardian, if the student has advanced beyond elementary school but has not yet reached the age of majority; or

(c) The student alone, if the student has reached the age of majority.

(3) An opt-in agreement shall not be valid if it actually or effectively grants a 1-to-1 device provider:

(a) General authority to access a student's 1-to-1 device; or

(b) The authority to collect all the student-generated content or data or personally identifiable student information that is generated by and/or used in connection with a specific program or application.

(4) An opt-in agreement may be revoked at any time, upon written notice to the educational institution or 1-to-1 device provider, by the person(s) eligible to authorize an opt-in agreement pursuant to Section 2(I)(2). Within 30 days of such a revocation, notice to any affected third parties shall be made by the educational institution or 1-to-1 device provider.

(5) The educational institution or 1-to-1 device provider that accesses, analyzes, or interacts with student-generated content or data or personally identifiable student information on a 1-to-1 device shall bear the burden of proving that it acted pursuant to a valid opt-in agreement.

(6) No 1-to-1 device program offered to an educational institution or its students may be conditioned upon the exclusive use of any software, application, website or Internet-based service sold or provided by the 1-to-1 device provider.

(7) No 1-to-1 device or related educational benefit may be withheld from, or punitive measure taken against, a student or the student's parent or legal guardian:

(a) Based in whole or in part upon a decision not to sign, or to revoke, an opt-in agreement; or

(b) Based in whole or in part upon a student's refusal to open, close, or maintain an email or other electronic communications or social media account with a specific service provider.

(8) A 1-to-1 device provider shall violate Section 2(I)(7)(a) if it conditions the offer, provision, or receipt of a 1-to-1 device upon a student's or the student's parent's or legal guardian's agreement to provide access to student-generated content or data or personally identifiable student information.

(J) Except as provided for in this Act, no educational institution, school employee, or 1-to-1 device provider may grant a person or entity access to review or interact with a 1-to-1 device or any of the data thereon unless required by statute, judicial warrant based on a probable cause standard, or court order, or as part of an audit initiated by an educational institution.

(K) When a 1-to-1 device is permanently returned by a student, the educational institution or 1-to-1 device provider who provided it shall, without otherwise accessing the student-generated content or data on the 1-to-1 device, fully erase all the data stored on the device and return the device to its default factory settings.

(L) The provisions of Section 2 that relate to the collection and use of student-generated content or data or personally identifiable student information shall not apply to student-generated content or data or personally identifiable student information collected by a 1-to-1 provider from a software program, website or application that was:

(1) Not pre-loaded on the 1-to-1 device;

(2) Not the target of a link that was pre-loaded on the 1-to-1 device; and

(3) Not promoted, marketed, or advertised in connection with the issuance of the 1-to-1 device.

Section 3 – Limitations on Use:

(A) Evidence or information obtained or collected in violation of this Act shall be promptly deleted and destroyed and shall not be admissible in any civil or criminal trial or legal proceeding, disciplinary action, or administrative hearing, or used by an educational institution for any other purpose.

Section 4 – Penalties:

(A) Any entity that violates this Act shall be subject to legal action for damages and/or equitable relief, to be brought by any other person claiming a violation of this Act has injured his or her person or reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured on account of violation of the provisions of this Act, and a reasonable attorney's fee and other costs of litigation.

(B) Any school employee or school enforcement official who violates this Act, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment. For school employees or school enforcement officials who are represented under the terms of a collective bargaining agreement, this Act prevails except where it conflicts with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.

Section 5 – Severability:

The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person, entity, or circumstance, is held invalid, the remainder of this Act, including the application of such part or provision to other persons, entities, or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 6 – Effective Date:

This Act shall take effect 180 days after passage.