AN ACT TO PROTECT STUDENT PRIVACY WITH RESPECT
TO ELECTRONIC DATA ON STUDENT INFORMATION SYSTEMS

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

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

(A) "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.

(B) "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(M).

(C) "Educational institution" shall mean:

(1) A private or public 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).

(D) "Educational record" shall mean educational record as defined by 20 U.S.C. §1232g(a)(4) on the date of this Act's adoption.

(E) "Education research" shall mean the systematic gathering of empirical information to advance knowledge, answer questions, identify trends, or improve outcomes within the field of education.

(F) "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.*).

Comment [CM1]: *NOTE TO AFFILIATES: Your state may already have a definition of this term, and you may opt to use that definition instead. This model bill was drafted in October 2015.*

(G) "Law enforcement official" shall mean an officer or employee of any agency or authority of the {state/commonwealth} of {State name}, or a political subdivision or agent thereof, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law, make arrests, and/or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

(H) "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, SIS provider, or 1-to-1 device provider with limited permission to access and interact with a specifically defined set of personally identifiable student information.

(I) "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 is capable of being de-aggregated or reconstructed to the point that individual students can be identified; and

(7) Any student 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.

Comment [CM2]: *NOTE TO AFFILIATES: Your state may already have a definition of this term, but **make sure** it includes state and local officers, but not federal.*

(J) "School employee" shall mean an individual who is employed by an educational institution, compensated through an annual salary or hourly wage paid by an educational institution, and whose services are primarily rendered at a physical location which is owned or leased by that educational institution. For purposes of this Act, individuals with law enforcement or school security responsibilities, including school resource officers, school district police officers, contract or private security companies, security guards, or other law enforcement personnel are not school employees.

(K) "SIS provider" shall mean an entity that sells, leases, provides, operates, or maintains a student information system for the benefit of an educational institution.

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

(M) "Student data" shall mean data that is collected and stored by an educational institution, or by a person or entity acting on behalf of that institution, and included in a student's educational record.

(N) "Student information system" or "SIS" shall mean a software application and/or cloud-based service that allows an educational institution to input, maintain, manage, and/or retrieve student data and/or personally identifiable student information, including applications that track and/or share personally identifiable student information in real time.

Comment [CM3]: *NOTE TO AFFILIATES: Your state may already have a definition of this term, but **make sure** it is limited to those who work on-site.*

Comment [CM4]: *NOTE TO AFFILIATES: Your state may already have a definition of this term.*

Section 2 – Student Information Systems:

(A) Any contract or other agreement between an educational institution and an SIS provider pursuant to which the SIS provider sells, leases, provides, operates, or maintains a student information system for the benefit of the educational institution:

(1) Shall expressly authorize and require the SIS provider to:

(a) Establish, implement and maintain appropriate security measures, consistent with best current practices, to protect the student data and personally identifiable student information the SIS provider creates, sends, receives, stores, and transmits in conjunction with the operation of the student information system;

(b) Acknowledge that no data stored on the student information system is the property of the SIS provider;

(c) Establish and implement policies and procedures for responding to data breaches involving the unauthorized acquisition of or access to any personally identifiable student information on the student information system. Such policies and procedures, at a minimum, shall:

(i) Require notice be provided by the SIS provider to any and all affected parties, including education institutions, students, and students' parents and legal guardians, within 30 days of the discovery of the breach;

(ii) Require the notice to include a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person;

(iii) Require the notice to provide a procedure by which affected parties may learn what types of sensitive personally identifiable information the SIS provider maintained about the affected individual; and

(iv) Satisfy all other applicable breach notification standards established under state or federal law.

(d) Permanently delete all data stored on the student information system, and destroy all non-digital records containing any personally identifiable student information retrieved from the student information system, within 90 days of the termination of the SIS provider's contact with the educational institution, except where the SIS provider and the person(s) authorized to sign a valid opt-in agreement pursuant to Section 2(B)(2) mutually agree the SIS provider will retain specifically identified data and/or non-digital records for the student's benefit.

(i) Prior to deletion, if requested by the educational institution, the terminated SIS provider shall transfer a designated portion or all of the data stored on the student information system to another designated SIS provider at the educational institution's expense.

(e) Comply with all the applicable obligations and restrictions established for SIS providers in this Act.

(2) Shall expressly prohibit the SIS provider from:

(a) Analyzing, interacting with, sharing, or transferring any student data or personally identifiable student information the educational institution inputs into or otherwise provides to the student information system unless:

(i) Permission to do so has been granted, pursuant to a Section 2(B) opt-in agreement;

(ii) The SIS provider analyzes or interacts with the student data or personally identifiable student information:

a. In order to meet a contractual obligation to the educational institution; and

b. Any analysis of or interaction with the data or information is limited to meeting that contractual obligation;

(iii) The SIS provider analyzes or interacts with the student data or personally identifiable student information:

a. In response to a specific request made by an educational institution; and

b. Any data or information produced as a result of the analysis or interaction is limited to the educational purpose for which it was sought;

(iv) The educational institution determines, and documents in writing, that sharing specific student data or personally identifiable student information is necessary to safeguard students' health and/or safety while students are traveling to or from the educational institution,

are on the educational institution's property, or are participating in an event or activity supervised by the educational institution; or

(v) At the request of the educational institution, the SIS provider de-identifies and/or aggregates student data or personally identifiable student information for the purpose of:

a. Enabling the educational institution to comply with federal, state and/or local reporting and data sharing requirements; or

b. Education research.

(vi) The data is accessed by the SIS provider for the exclusive purpose of testing and improving the value and performance of its student information system for the benefit of the educational institution.

a. Where data is accessed to test and improve student information system value and performance:

i. Any copied data shall be permanently deleted within 60 days of the date the copy was created; and

ii. Any data analysis that contains personally identifiable student information shall be permanently deleted within 60 days of the date the analysis was created.

(b) Selling any student data or personally identifiable student information stored on or retrieved from the student information system unless it is sold as part of a sale or merger of the entirety of the SIS provider's business.

(i) Upon such a sale or merger, the provisions of this Act, and any relevant contracts or agreements, shall apply fully to the new purchasing or controlling person or entity.

(c) Using any student data or personally identifiable student information stored on or retrieved from the student information system to inform, influence or guide 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.

(d) Using any student data or personally identifiable student information stored on or retrieved from the student information system to develop, in full or in part, a profile of a student or group of students for any commercial or other non-educational purposes.

(B) Opt-In Agreements

(1) A valid opt-in agreement shall identify, with specificity:

(a) The precise subset of personally identifiable student information in the student information system (e.g., student attendance records, student disciplinary records) as to which the SIS provider is being granted authority to access, analyze, interact with, share and/or transfer;

(b) The name of the SIS provider(s) to whom the authority to access, analyze, interact with, share and/or transfer personally identifiable student information in the student information system is being granted;

(c) The educational purpose(s) for which the authority to access, analyze, interact with, share and/or transfer personally identifiable student information is being granted; 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 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) A valid opt-in agreement may authorize an SIS provider to share or transfer personally identifiable student information to another person or entity only where:

(a) The purpose of the transfer of the personally identifiable student information is to benefit:

(i) The operational, administrative, analytical, or educational functions of the educational institution, including education research; or

(ii) The student's education.

(b) The subset of personally identifiable student information to be shared or transferred is identified with specificity in the opt-in agreement;

(c) The person or entity to whom the personally identifiable student information is being shared or transferred is identified with specificity in the opt-in agreement;

(d) The benefit to the educational institution or student is identified with specificity in the opt-in agreement; and

(e) For each student, a record of what specific personally identifiable student information pertaining to that student was shared and/or transferred, when it was shared and/or transferred, and with whom it was shared and/or transferred is appended to the student's record.

(4) Any person or entity that accesses or takes possession of any student data or personally identifiable student information pursuant to Section 2(A)(2)(a)(i) or Section 2(A)(2)(b) shall be subject to same restrictions and obligations under this Section as the SIS provider from which the student data and/or personally identifiable student information was obtained.

(5) An opt-in agreement shall not be valid if it grants general authority to access, analyze, interact with, share and/or transfer a student's personally identifiable student information in a student information system.

(6) Except as authorized in this Section, no SIS provider, school employee, or other person or entity who receives personally identifiable student information, directly or indirectly, from a student information system pursuant to an opt-in agreement may share, sell or otherwise transfer such information to another person or entity.

(7) An opt-in agreement may be revoked at any time, upon written notice to an educational institution, by the person(s) eligible to authorize an opt-in agreement

pursuant to Section 2(B)(2). Within 30 days of such a revocation, notice to the SIS provider shall be provided by the educational institution.

(8) An SIS provider that accesses, analyzes, interacts with, shares and/or transfers personally identifiable student information to another person or entity shall bear the burden of proving that it acted pursuant to a valid opt-in agreement.

(9) No educational benefit may be withheld from, or punitive measure taken against, a student or the student's parent or legal guardian based in whole or in part upon a decision not to sign, or to revoke, an opt-in agreement.

(C) School employees

(1) Subject to written authorization from the educational institution, school employees may access and interact with student data and personally identifiable student information on a student information system in furtherance of their professional duties.

(a) Notwithstanding any other provisions in this Section, no school employee may receive authorization to access and interact with student data or personally identifiable student information on a student information system until the employee has received adequate training to ensure the school employee's understanding and compliance with the provisions of this Section.

(2) School employees may not sell, share, or otherwise transfer student data or personally identifiable student information to another person or entity, except:

(a) Where specifically authorized to do so pursuant to this Section;

(b) With the educational institution that employees the school employee;

(c) With another school employee who is eligible to access such information pursuant to Section 2(C)(1); and

(d) Where:

(i) The school employee is a teacher;

(ii) The teacher is transferring student data to a software application for classroom recordkeeping and/or management purposes only;

(iii) Any third parties with access to the software application are expressly prohibited from reviewing or interacting with the transferred data; and

(iv) Any data transferred to the software application by the teacher is deleted by the teacher within 45 days of such time as it is no longer being actively used for classroom recordkeeping and/or management purposes.

(D) A student's parent or guardian, upon written request to an educational institution, shall be permitted to inspect and review their child's student data and personally identifiable student information that is stored on a student information system. Educational institutions shall afford parents and legal guardians a reasonable and fair opportunity to request corrections to or seek removal of inaccurate data.

(1) The right of a student's parent or guardian to review their child's student data and personally identifiable student information shall not apply where:

(a) Such information was supplied by the child to the educational institution; and

(b) There is a reasonable likelihood the disclosure of such information would generate a threat to the student's health and/or safety.

(2) The right of a student's parent or guardian to review their child's student data and personally identifiable student information shall not apply where access to particularly specified information has been waived by the student or the student's parent or guardian.

(3) When a student reaches the age of majority, the rights granted to a student's parents and legal guardian pursuant to Section 2(D) shall terminate, and instead shall vest with the student.

(4) An educational institution shall establish appropriate procedures for:

(a) Reviewing and responding to requests made pursuant to Section 2(D) within 30 days of its receipt of the request; and

(b) Requesting and receiving a fair hearing in the event a requested correction is denied.

(E) One year after a student's graduation, withdrawal, or expulsion from an educational institution, all student data and personally identifiable student information related to that student that is stored in a student information system shall be deleted.

(1) This provision shall not apply to:

(a) A student's name and social security number;

(b) A student's transcript, graduation record, letters of recommendation, and other information required by an institution of higher education for an application for admission or by a potential employer for an application for employment;

(c) Student data and personally identifiable student information that is the subject of an ongoing disciplinary, administrative, or judicial action or proceeding;

(d) De-identified student data that is being retained at the request of the educational institution for the purpose of educational research and/or analysis; and

(e) Student data or personally identifiable student information where its retention is otherwise required by law or a judicial order or warrant.

(F) Within 180 days of receiving notification, pursuant to Section 2(G), of a student's graduation, withdrawal, or expulsion from an educational institution, all physical or digital copies of any student data and personally identifiable student information related to the student that was obtained from a student information system and is in the possession or under the control of an SIS provider or other third party shall be deleted or destroyed.

(1) This provision shall not apply to:

(a) Student data and personally identifiable student information that is the subject of an ongoing disciplinary, administrative, or judicial action or proceeding;

(b) Aggregated and/or de-identified student data obtained for the purpose of education research;

(c) Student data or personally identifiable student information where its retention is otherwise required by law or a judicial order or warrant; and

(d) Specifically identified student data or personally identifiable student information, where:

(i) Its retention is requested by the person(s) authorized to sign a valid opt-in agreement pursuant to Section 2(B)(2); and

(ii) The SIS provider and educational institution voluntarily consent to its retention.

(G) Within 90 days of a student's graduation, withdrawal, or expulsion from an education institution, notice of such shall be provided by the educational institution to the SIS provider, which shall in turn notify any third parties with whom the SIS provider shared the student's student data and/or personally identifiable student information.

(H) No person or entity, other than an educational institution, school employee or SIS provider, other than as provided for in this Section, shall be granted access to review or interact with a student information system and the data thereon, unless otherwise authorized to do so by law, pursuant to a judicial warrant, or as part of an audit initiated by an educational institution.

(I) Nothing in the Section shall be read to prohibit an educational institution from providing directory information to a vendor for the express purpose of providing photography services, class ring services, yearbook or student publication publishing services, memorabilia services, or similar services, provided the vendor agrees in writing:

(1) Not to sell or transfer the data to any other persons or entities;

(2) To use the data solely for the express purpose for which it was provided; and

(3) To destroy the data upon completion of its use for the express purpose it was provided.

(J) Nothing in this Section shall be read to supersede or otherwise limit any laws that provide enhanced privacy protections to students or further restrict access to their educational records or personally identifiable student information.

Section 3 – Limitations on Use:

(A) Evidence or information obtained or collected in violation of this Act shall not be admissible in any civil or criminal trial or legal proceeding, disciplinary action, or administrative hearing.

Section 4 – Penalties:

(A) Any person or entity who 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 who violates this Act, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment. For school employees 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.