

STATE OF KANSAS

SENATE CHAMBER

MADAM PRESIDENT:

I move to amend **SB 367**, as amended by Senate Committee, on page 1, by striking all in lines 4 through 35; in line 36,

By striking all on page 2 and 3 and inserting:

"Section 1. Sections 1 through 11, and amendments thereto, shall be known and may be cited as the student and teacher data privacy act.

Sec. 2. As used in sections 1 through 11, and amendments thereto:

(a) "Biometric data" means one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual, such as fingerprints, retina and iris patterns, voice prints, DNA sequence, facial characteristics and handwriting.

(b) "Aggregate data" means data collected or reported at the group, cohort or institutional level.

(c) "De-identified data" means a student dataset in which personally identifiable information has been removed.

(d) "Department" means the state department of education.

(e) "Educational agency" means a school district, the department or a postsecondary educational institution.

(f) "Postsecondary educational institution" shall have the same meaning as that term is defined in K.S.A. 74-3201b, and amendments thereto.

(g) "School district" means a unified school district organized and operated under the laws of this state.

(h) "Statewide longitudinal student data system" means any student data system maintained by the department, which assigns a state identification number for each student who attends an accredited public or private school in Kansas and uses the state identification number to collect student data.

(i) "Personally identifiable information" includes:

- (1) Parent, student or teacher identifying information, such as name, address or date of birth;
- (2) a student's or teacher's state identification number; and
- (3) any other information that, alone or in combination with other information, is connected to a specific student or teacher that would allow a reasonable person to identify a student or teacher with reasonable certainty.

(j) "State board" means the state board of education.

(k) "Student data" means data collected or reported at the individual student level in a student's educational record and includes, but is not limited to:

- (1) State and national assessment results, including information on untested students;
- (2) courses taken and completed, credits earned and other transcript information;
- (3) course grades and grade point average;
- (4) grade level and expected date of graduation;
- (5) degree, diploma, credential attainment, and other school exit information such as general education development and drop-out data;
- (6) attendance and mobility;
- (7) data required to calculate the federal four-year adjusted cohort graduation rate, including sufficient exit and drop-out information;
- (8) discipline reports limited to objective information sufficient to produce any reports that are required to receive federal title IV funding;

(9) remediation;

(10) special education data;

(11) demographic data such as date of birth, place of birth, residential address, social security numbers; and

(12) any other information included in a student's educational record.

(l) "Teacher data" means data collected or reported at the individual teacher level in a teacher's educational record and includes:

(1) Courses taken and completed in college, credits earned, date of graduation and other transcript information;

(2) courses and grade levels taught in K-12 schools;

(3) date of birth, place of birth, residential address or social security number;

(4) degree, diploma, credential attainment, and other teacher licensure information; and

(5) names and addresses of schools in which the teacher has taught.

Sec. 3. No school district shall collect biometric data from a student or teacher, or use any device or mechanism to assess a student's or teacher's physiological or emotional state, unless the student, if an adult, or the parent or legal guardian of the student, if a minor, or the teacher first signs a written consent.

Sec. 4. (a) On and after July 1, 2014, neither the state board, the department, nor any other state agency shall:

(1) Expend any funds, whether from federal grants, funds provided by the American recovery and reinvestment act of 2009 (Pub. L. 111-5), funds appropriated from the state general fund or from any other source, on the construction, enhancement, or expansion of any state-wide longitudinal student data system; or

(2) share or provide access to any aggregate data compiled on students or teachers with any

entity outside the state of Kansas, except as provided in subsection (b).

(b) The state board shall use only aggregate data in its reporting:

(1) To any federal agency, state or local agency inside or outside the state of Kansas, or any other in-state or out-of-state organization or entity;

(2) in its public reports; or

(3) in response to record requests.

(c) Only local school districts may compile personally identifiable student and nonacademic family information which is necessary either for administrative functions directly related to the student's education, for evaluation of academic programs and student progress, or for compliance with the requirements of the United States department of education as outlined in subsection (f).

(d) In compliance with K.S.A. 72-6214(b)(2), and amendments thereto, no personally identifiable student or teacher data shall be released to any local, state or federal agency, contractor or researcher by any local school district without first receiving the written consent of the student's parent or guardian or the affected teacher.

(e) (1) Except as provided by paragraph (2), any student and teacher data and de-identified data maintained by the department is confidential.

(2) A local school district may transfer student or teacher level data to any federal agency, state or local agency inside or outside the state of Kansas, or any other out-of-state organization or entity in the following circumstances:

(i) An adult student, a minor student's parent or guardian or a teacher first requests, in writing, that their personally identifiable data be transferred to an in-state or out-of-state school district or postsecondary educational institution;

(ii) a student or teacher registers for or takes a national assessment or certification test;

(iii) an adult student, a minor student's parent or guardian or a teacher voluntarily agrees in

writing to participate in a program for which such a data transfer is a requirement of participation.

(f) Student or teacher aggregate data, but not personally identifiable, student-level or teacher-level data may be shared by a local school district, the state board or the department with the United States department of education only when:

(1) Such sharing or access provided is required by the United States department of education as a condition of receiving a federal education grant;

(2) the United States department of education agrees in writing to use the data only to evaluate the program or programs funded by the grant;

(3) the United States department of education agrees in writing that the data will not be used for any research beyond that related to evaluation of the program or programs funded by the grant, unless the parent or guardian of any student, and any teacher, whose data will be used for such research affirmatively consents in writing to that use;

(4) the United States department of education agrees in writing to destroy or return to the state agency, local school district board, or educational agency all personally identifiable information in its custody upon request and at the termination of the contract. Destruction shall be compliant with the NISTPS800-88 standards of data destruction; and

(5) the grant or program in connection with which the data are required is one authorized by federal statute or by federal rule properly promulgated under the federal administrative procedure act, 5 U.S.C. § 500 et seq.

Sec. 5. No test, questionnaire, survey, or examination containing any questions about the student's personal beliefs or practices on issues such as sex, family life, morality and religion, or any questions about the student's parents' or guardians' beliefs and practices on issues such as sex, family life, morality, and religion, shall be administered to any student in kindergarten or grades one to 12, inclusive, unless the parent or guardian of the student is notified in writing that this test, questionnaire,

survey or examination is to be administered and the parent or guardian of the student gives written permission for the student to take this test, questionnaire, survey, or examination.

Sec. 6. Any student results or a record of accomplishment shall be private, and may not be released to any person, other than the student's parent or guardian and a teacher, counselor or administrator directly involved with the student, without the express written consent of either the parent or guardian of the student if the student is a minor, or the student if the student has reached the age of majority or is emancipated.

Sec. 7. No test, examination, or assessment given as part of the statewide student assessment program shall contain any questions or items that solicit or invite disclosure of a student's or such student's parents' or legal guardians' personal beliefs or practices in sex, family life, morality or religion nor shall it contain any question designed to evaluate personal behavioral characteristics, including, but not limited to, honesty, integrity, sociability or self-esteem.

Sec. 8. Notwithstanding any other provision of law, a parent's or guardian's written request to school officials to excuse such parent's or legal guardian's child from any or all parts of the Kansas state assessments shall be granted.

Sec. 9. (a) State agencies, local school boards and institutions shall not disclose personally identifiable information from education records or teacher records without the prior written consent of parents or eligible students or of the affected teachers, to a contractor, consultant, or other party to whom the state agency, school board, or institution has outsourced institutional services or functions. If and when written consent is provided by the research subjects, the outside party must certify in writing that it:

- (1) Performs an institutional service or function for which the state agency, school board, or institution would otherwise use its employees;
- (2) is under the direct control of the state agency, school board, or institution with respect to

the use and maintenance of education records or teacher records;

(3) limits internal access to education records or teacher records to those individuals who require access to those records for completion of the contract;

(4) does not use the education records or teacher records for any purposes other than those explicitly authorized in the contract;

(5) does not disclose any personally identifiable information from education records or teacher records to any other party:

(A) Without the written consent of the parent or eligible student, or the affected teacher; or

(B) unless required by statute or court order and the party provides a notice of the disclosure to the state agency, school board or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

(6) maintains reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of the personally identifiable student or teacher data in its custody;

(7) uses encryption technologies to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the United States department of health and human services in guidance issued under section 13402(H)(2) of the American recovery ad reinvestment act (Pub. L. 111-5);

(8) has sufficient administrative and technical procedures to monitor continuously the security of personally identifiable student or teacher data in its custody;

(9) conducts a security audit annually and provides the results of that audit to each state agency, school board or institution that provides education records or teacher records;

(10) provides the state agency, school board or institution with a breach-remediation plan

acceptable to the state agency, school board, or institution before initial receipt of education records or teacher records. Results of these audits need to be accessible by the parents or legal guardians of the students or teachers;

(11) reports all suspected security breaches to the state agency, school board or institution that provided education records or teacher records as soon as possible but not later than 48 hours after a suspected breach was known or would have been known by exercising reasonable diligence, as well as parents or legal guardians of students or any other victim connected with the suspected security breach;

(12) reports all actual security breaches to the state agency, school board or institution that provided education records as soon as possible but not later than 24 hours after an actual breach was known or would have been known by exercising reasonable diligence and reports such breach to the parents or legal guardians of students, affected teachers or any other victim connected with the suspected security breach;

(13) in the event of a security breach or unauthorized disclosure of personally identifiable information, pays all costs and liabilities incurred by the state agency, school board or institution related to the security breach or unauthorized disclosure, including, but not limited to, the costs of responding to inquiries about the security breach or unauthorized disclosure, of notifying subjects of personally identifiable information about the breach, of mitigating the effects of the breach for the subjects of the personally identifiable information and of investigating the cause or consequences of the security breach or unauthorized disclosure; and

(14) destroys or returns to the state agency, school board or institution all personally identifiable information in its custody upon request and at the termination of the contract. Destruction shall be compliant with the NISTPS800-88 standards of data destructions.

Sec. 10. In the event of a security breach or unauthorized disclosure of personally identifiable student or teacher data, whether by a state agency, school board or educational institutional, or by a

third party given access to education records or teacher records, the state board, department, state agency, local school board or educational institution shall:

- (a) Immediately notify the subjects of the breach or disclosure;
- (b) report the breach or disclosure to the family policy compliance office of the United States department of education; and
- (c) investigate the causes and consequences of the breach or disclosure.

Sec. 11. The attorney general or any district attorney may enforce the provisions of sections 1 through 10, and amendments thereto, by investigating and bringing an action in a court of competent jurisdiction, and may seek injunctive relief to enjoin any educational agency, any employee or agent thereof, or any other entity in possession of student or teacher data from disclosing any student or teacher data in violation of the provisions of sections 1 through 10, and amendments thereto. To carry out such investigation, the attorney general or any deputy or assistant attorney general is authorized to subpoena witnesses, compel their attendance, examine them under oath, and require that any books, records, documents, papers, or electronic records relevant to the inquiry be turned over for inspection, examination, or audit.

Sec. 12. This act shall take effect and be in force from and after its publication publication in the statute book.";

On page 1, in the title, in line 1, after "student" by inserting "and teacher"

Senator _____