1

2

3

4 5

6

7

8

9 10

11

12

13

14 15

16

17

18 19

20

21

22

23

24

25

26

27 28

29 30

31

32 33

34 35

36

37

38

39 40

IN THE SENATE

SENATE BILL NO. 1296

BY EDUCATION COMMITTEE

AN ACT RELATING TO EDUCATION; TO PROVIDE A SHORT TITLE; TO PROVIDE LEGISLATIVE INTENT; AMENDING CHAPTER 1, TITLE 33, IDAHO CODE, BY THE ADDITION OF A NEW SECTION 33-133, IDAHO CODE, TO PROVIDE DEFINITIONS, TO PROVIDE FOR A RESPONSIBLE ENTITY, TO ESTABLISH PROVISIONS RELATING TO A DATA INVENTORY AND DICTIONARY OR INDEX, TO ESTABLISH PROVISIONS RELATING TO CERTAIN POLICIES AND PROCEDURES, TO ESTABLISH PROVISIONS RELATING TO THE STATE BOARD OF EDUCATION AND THE STATE DEPARTMENT OF EDUCATION EN-SURING THAT CERTAIN VENDORS SHALL COMPLY WITH THE LAW, TO PROVIDE FOR A CIVIL ENFORCEMENT ACTION, TO PROVIDE FOR A COURT ACTION, TO PROVIDE FOR A PENALTY, TO ESTABLISH PROVISIONS RELATING TO DATA DEEMED CONFIDEN-TIAL, TO PROVIDE FOR EXCEPTIONS, TO PROVIDE FOR A DATA SECURITY PLAN, TO ESTABLISH PROVISIONS RELATING TO COMPLIANCE WITH CERTAIN POLICIES AND LAWS, TO ESTABLISH PROVISIONS RELATING TO CERTAIN CONTRACTS, TO PRO-VIDE FOR NOTIFICATION TO THE GOVERNOR AND THE LEGISLATURE, TO PROVIDE FOR RULES, TO ESTABLISH PROVISIONS RELATING TO EXISTING COLLECTION OF

Be It Enacted by the Legislature of the State of Idaho:

SECTION 1. SHORT TITLE. This act shall be known as the "Student Data Accessibility, Transparency and Accountability Act of 2014."

AND TO PROVIDE FOR PENALTIES; AND DECLARING AN EMERGENCY.

STUDENT DATA, TO ESTABLISH PROVISIONS RELATING TO A PARENT OR GUARDIAN

REQUEST FOR THEIR CHILD'S STUDENT RECORD, TO PROVIDE FOR A MODEL POLICY

SECTION 2. LEGISLATIVE INTENT. It is the intent of the Legislature to help ensure that student information is safequarded and that privacy is honored, respected and protected. The Legislature also acknowledges that student information is a vital resource for teachers and school staff in planning responsive education programs and services, scheduling students into appropriate classes and completing reports for educational agencies. Student information is critical in helping educators assist students in successfully graduating from high school and being ready to enter the workforce or postsecondary education. In emergencies, certain information should be readily available to school officials to assist students and their families. A limited amount of this information makes up a student's permanent record or transcript. The Legislature firmly believes that while student information is important for educational purposes, it is also critically important to ensure that student information is protected, safeguarded and kept private and used only by appropriate educational authorities and then, only to serve the best interests of the student. To that end, this act will help ensure that student information is protected and expectations of privacy are honored.

SECTION 3. That Chapter 1, Title 33, Idaho Code, be, and the same is hereby amended by the addition thereto of a <u>NEW SECTION</u>, to be known and designated as Section 33-133, Idaho Code, and to read as follows:

- 33-133. DEFINITIONS -- STUDENT DATA -- USE AND LIMITATIONS. (1) As used in this act, the following terms shall have the following meanings:
 - (a) "Agency" means each state board, commission, department, office or institution, educational or otherwise, of the state of Idaho. State agency shall also mean any city, county, district or other political subdivision of the state.
 - (b) "Aggregate data" means data collected and/or reported at the group, cohort or institutional level. The minimum number of students shall be determined by the state board of education.
 - (c) "Board" means the state board of education.

- (d) "Data system" means the state department of education's Idaho system for educational excellence (ISEE) and also the state postsecondary longitudinal data system.
- (e) "Department" means the state department of education.
- (f) "District" or "school district" means an Idaho public school district and shall also include Idaho public charter schools.
- (g) "Personally identifiable data," "personally identifiable student data" or "personally identifiable information" includes, but is not limited to: the student's name; the name of the student's parent or other family members; the address of the student or student's family; a personal identifier, such as the student's social security number, student education unique identification number or biometric record; other indirect identifiers, such as the student's date of birth, place of birth and mother's maiden name; and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.
- (h) "Provisional student data" means new student data proposed for inclusion in the data system.
- (i) "Student data" means data collected and/or reported at the individual student level included in a student's educational record.
 - (i) "Student data" includes: (1) state and national assessment results, including information on untested public school students; (2) course taking and completion, credits earned and other transcript information; (3) course grades and grade point average; (4) date of birth, grade level and expected graduation date/graduation cohort; (5) degree, diploma, credential attainment and other school exit information such as general educational development and drop-out data; (6) attendance and mobility; (7) data required to calculate the federal four (4) year adjusted cohort graduation rate, including sufficient exit and drop-out information; (8) discipline reports limited to objective information sufficient to produce the federal annual incident reports,

children with disabilities disciplinary reports and discipline reports including students involved with firearms; (9) remediation; (10) special education data; (11) demographic data and program participation information; and (12) files, documents, images or data that are stored in or transmitted through a cloud computing service.

- (ii) Unless included in a student's educational record, "student data" shall not include: (1) juvenile delinquency records; (2) criminal records; (3) medical and health records; (4) student social security number; (5) student biometric information; (6) gun ownership records; (7) sexual orientation; and (8) religious affiliation.
- (j) "Student educational record" means all information directly related to a student and recorded and kept in the data system as that term is defined in this section. A student educational record may include information considered to be personally identifiable.
- (k) "Student education unique identification number" means the unique student identifier assigned by the state to each student that shall not be or include the social security number of a student in whole or in part.
- (2) Unless otherwise provided for in this act, the executive office of the state board of education shall be the entity responsible for implementing the provisions of this act. All decisions relating to the collection and safeguarding of student data shall be the responsibility of the executive office of the state board of education.
 - (3) The state board of education shall:

- (a) Create, publish and make publicly available a data inventory and dictionary or index of data elements with definitions of individual student data fields currently in the student data system including:
 - (i) Any individual student data required to be reported by state and federal education mandates;
 - (ii) Any individual student data that has been proposed for inclusion in the student data system with a statement regarding the purpose or reason for the proposed collection; and
 - (iii) Any individual student data collected or maintained with no current purpose or reason.

No less frequently than annually, the state board of education shall update the data inventory and index of data elements provided for in this subsection.

- (b) Develop, publish and make publicly available policies and procedures to comply with the federal family educational rights and privacy act (FERPA) and other relevant privacy laws and policies including, but not limited to:
 - (i) Access to student data in the student data system shall be restricted to: (1) the authorized staff of the state board of education and the state department of education and the board's and the department's vendors who require such access to perform their assigned duties; (2) district and public postsecondary staff who require such access to perform their assigned duties; (3) students and their parents or legal guardians; and (4) the authorized staff

of other state agencies in this state as required by law and/or defined by interagency data-sharing agreements;

- (ii) Public reports or responses to record requests shall include aggregate data only as that term is defined in subsection (1) of this section;
- (iii) The state board of education shall develop criteria for the approval of research and data requests from state and local agencies, the state legislature, researchers and the public: (1) unless otherwise approved by the state board of education, student data maintained shall remain confidential; (2) unless otherwise approved by the state board of education, released student data in response to research and data requests may only include aggregate data; and (3) any approval of the board to release personally identifiable student data shall be subject to legislative approval prior to the release of such information;
- (iv) Ensuring that any contract entered into by the state board of education or the state department of education includes provisions requiring and governing data destruction dates and specific restrictions on the use of data;
- (v) Notification to students and parents regarding their rights under federal and state law; and
- (vi) Ensuring that all school districts, primary schools, secondary schools and other similar institutions entering into contracts that govern databases, online services, assessments, special education or instructional supports with private vendors shall include in each such contract either: (1) a prohibition on any secondary uses of student data by the private vendor including, but not limited to, sales, marketing or advertising, but permitting the private vendor to process or monitor such data solely to provide and maintain the integrity of the service; or (2) a requirement that the private vendor disclose in detail any secondary uses of student data including, but not limited to, sales, marketing or advertising, and the board shall obtain express parental consent for those secondary uses prior to deployment of the private vendor's services under the contract.

The state board of education and the state department of education shall ensure that any and all private vendors employed or otherwise engaged by the board or the department shall comply with the provisions of this section. Any person determined, in either a civil enforcement action initiated by the board or initiated by the department or in a court action initiated by an injured party, to have violated any provision of this section or any rule promulgated pursuant to this section, shall be liable for a civil penalty not to exceed fifty thousand dollars (\$50,000) per violation. In the case of an unauthorized release of student data, the state board of education or the state department of education shall notify the parent or student of the unauthorized release of student data that includes personally identifiable information in a manner consistent with the provisions of section 28-51-105, Idaho Code.

(c) Unless otherwise approved by the state board of education, any data deemed confidential pursuant to this act shall not be transferred to any

federal, state or local agency or other organization or entity outside of the state of Idaho, with the following exceptions:

- (i) A student transfers out of state or a school or district seeks help with locating an out-of-state transfer;
- (ii) A student leaves the state to attend an out-of-state institution of higher education or training program;
- (iii) A student voluntarily participates in a program for which such a data transfer is a condition or requirement of participation;
- (iv) The state board of education or the state department of education may share such data with a vendor to the extent it is necessary as part of a contract that governs databases, online services, assessments, special education or instructional supports with a vendor;
- (v) Pursuant to a written agreement between the two (2) school districts, where a student transfers from an Idaho district abutting upon another state to the nearest appropriate district in such neighboring state in accordance with the provisions of section 33-1403, Idaho Code; or
- (vi) A student is classified as "migrant" for federal reporting
 purposes;
- (d) Develop a detailed data security plan that includes:
 - (i) Guidelines for authorizing access to the student data system and to individual student data including guidelines for authentication of authorized access;
 - (ii) Guidelines relating to administrative safeguards providing for the security of electronic and physical data; such guidelines should include provisions relating to data encryption as well as staff training to better ensure the safety and security of data;
 - (iii) Privacy compliance standards;
 - (iv) Privacy and security audits;

- (v) Breach planning, notification and procedures; and
- (vi) Data retention and disposition policies;
- (e) Ensure routine and ongoing compliance with FERPA, other relevant privacy laws and policies, and the privacy and security policies and procedures developed under the authority of this act, including the performance of compliance audits;
- (f) Ensure that any contracts that govern databases, online services, assessments or instructional supports that include student data and are outsourced to private vendors, include express provisions that safeguard privacy and security, contain the restrictions on secondary uses of student data described in subsection (3)(b)(vi) of this section, provides for data destruction and includes penalties for noncompliance with this paragraph; and
- (g) Notify the governor and the legislature annually of the following:
 - (i) New student data proposed for inclusion in the state student data system: (1) any new student data collection proposed by the state board of education becomes a provisional requirement to allow districts and their local data system vendors the opportunity to meet the new requirement; and (2) the state board of educa-

tion must submit any new provisional student data collection to the governor and the legislature for their approval within one (1) year in order to make the new student data a permanent requirement through the administrative rules process. Any provisional student data collection not approved by the governor and the legislature by the end of the next legislative session expires and must be deleted and no longer collected;

- (ii) Changes to existing data collections required for any reason, including changes to federal reporting requirements made by the U.S. department of education;
- (iii) An explanation of any exceptions granted by the state board of education in the past year regarding the release or out-of-state transfer of student data;
- (iv) The results of any and all privacy compliance and security audits completed in the past year. Notifications regarding privacy compliance and security audits shall not include any information that would pose a security threat to the state or local student information systems or to the secure transmission of data between state and local systems by exposing vulnerabilities; and
- (v) Data collected specific to a grant program where such data is not otherwise included in student data.
- (4) The state board of education shall adopt rules to implement the provisions of this act.
- (5) Upon the effective date of this act, any existing collection of student data in the data system shall not be considered a new student data collection in accordance with this section.
- (6) Unless otherwise prohibited by law or court order, school districts must provide parents or guardians with copies of all of their child's educational records, upon request, if such child has not attained the age of eighteen (18) years.
- (7) The state board of education shall develop a model policy for school districts and public charter schools that will govern data collection, access, security and use of such data. The model policy shall be consistent with the provisions of this act. In order to assure that student educational information is treated safely and securely and in a consistent manner throughout the state, each district and public charter school shall adopt and implement the model policy. The state department of education shall provide outreach and training to the districts and public charter schools to help implement the policy. A current copy of such policy shall be posted to the school district's website. Any district or public charter school that fails to adopt, implement and post the policy where any inappropriate release of data occurs shall be liable for a civil penalty not to exceed fifty thousand dollars (\$50,000). The method of recovery of the penalty shall be by a civil enforcement action brought by the state board of education, with the assistance of the office of the state attorney general, in the district court in and for the county where the violation occurred. All civil penalties collected under this section shall be paid into the general fund of the state.

SECTION 4. An emergency existing therefor, which emergency is hereby declared to exist, this act shall be in full force and effect on and after its passage and approval.