

SECOND REGULAR SESSION

HOUSE BILL NO. 1873

97TH GENERAL ASSEMBLY

INTRODUCED BY REPRESENTATIVES GUERNSEY (Sponsor), ANDERSON, NEELY, MORRIS, SPENCER, KELLEY (127), HOUGHTON, JONES (50), BAHR, REMOLE, HICKS, DOHRMAN, CURTMAN, ALLEN, MCGAUGH, DAVIS, CROSS, KORMAN, COX, MOON, FITZWATER, KOENIG, REHDER, SHUMAKE, HANSEN, MESSENGER, REIBOLDT, KEENEY, WIELAND, POGUE, MOLENDORP, HAAHR, LANT, SWAN, WALKER AND FITZPATRICK (Co-sponsors).

5517L.04I

D. ADAM CRUMBLISS, Chief Clerk

AN ACT

To amend chapter 160, RSMo, by adding thereto seven new sections relating to student data privacy, with an emergency clause and a penalty provision.

Be it enacted by the General Assembly of the state of Missouri, as follows:

Section A. Chapter 160, RSMo, is amended by adding thereto seven new sections, to be known as sections 160.2510, 160.2512, 160.2514, 160.2516, 160.2518, 160.2520, and 160.2522, to read as follows:

160.2510. 1. The provisions of sections 160.2510 to 160.2522, which shall take effect beginning with the 2014-15 school year, shall be known and referred to as the "Missouri Student Data Protection Act". For purposes of sections 160.2510 to 160.2522, the following terms mean:

(1) "Affective computing", systems and devices that can or attempt to recognize, interpret, process, or simulate aspects of human feelings or emotions;

(2) "Biometric records", any record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual, including fingerprints; retina and iris patterns; voiceprints; DNA sequence, including newborn screening information; facial characteristics; and handwriting;

(3) "Cloud computing service", a service that enables on-demand network access to a shared pool of configurable computing resources, including networks, servers, storage, applications, and services, to provide a student, teacher, or staff member account-based

EXPLANATION — Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted from the law. Matter in **bold-face** type in the above bill is proposed language.

14 productivity applications such as email, document storage and document editing that can
15 be rapidly provisioned and released with minimal management effort, or cloud computing
16 service provider interaction;

17 (4) "Data system", the Missouri Student Information System (MOSIS), or any
18 other data warehouse or repository containing student information, including regional,
19 interstate, or federal data warehouse organizations under contract or with a memorandum
20 of understanding with the Missouri department of elementary and secondary education;

21 (5) "Educational institution", any public elementary or secondary school, school
22 district, or school board;

23 (6) "Predictive modeling", the use of educational data mining methods to make
24 predictions about future behaviors or performance;

25 (7) "Public education agency", the Missouri department of elementary and
26 secondary education, the state board of education, the P-20 Council, the coordinating
27 board for early childhood education, or any regional elementary and secondary education
28 service agency;

29 (8) "Student performance data", information about the academic progress of a
30 single student, such as formative and summative assessment data, course work, instructor
31 observations, information about student engagement and time on task, and similar
32 information;

33 (9) "Teacher records", shall apply to teachers, paraprofessionals, principals, and
34 other administrators, and includes Social Security number, name, address, birth date,
35 email address, telephone number, compensation information, resume information,
36 performance evaluations, and any other information that, alone or in combination, is
37 linked or linkable to a specific staff member that would allow a reasonable person in the
38 school community who does not have personal knowledge of the relevant circumstances to
39 identify the staff member with reasonable certainty;

40 (10) "Workforce information", information relating to unemployment insurance,
41 wage records, unemployment insurance benefit claims, or employment and earnings data
42 from workforce data sources such as state wage records, the Wage Record Interchange
43 System (WRIS), or the federal Employment Data Exchange System (FEDES).

44 2. It shall be unlawful for any public education agency or educational institution
45 to collect without the informed written consent of a parent or guardian of a student, or in
46 the case of an emancipated minor the informed written consent of the student, any of the
47 following information:

48 (1) Student or family workforce information as defined in this section, except as
49 provided in subdivision (14) of subsection 3 of this section;

- 50 (2) Student biometric records, as defined in this section;
- 51 (3) Any data collected through affective computing as defined in this section,
52 including analysis of facial expressions, EEG brain wave patterns, skin conductance,
53 galvanic skin response, heart rate variability, pulse, blood volume, posture, and eye
54 tracking;
- 55 (4) Any data, including any resulting from state or national assessments, that
56 measure psychological resources, mindsets, learning strategies, effortful control, attributes,
57 dispositions, social skills, attitudes, or intrapersonal resources;
- 58 (5) Any data collected through predictive modeling, as defined in this section;
- 59 (6) Information about student or family religious affiliation;
- 60 (7) Medical, health, and mental health records limited to immunization records
61 required under state law, records needed or created by a school-based health professional
62 for administering prescription drugs or otherwise treating a student at school, records
63 needed or created by a school-based counselor when a student seeks counseling while at
64 school, or records required by the Individuals with Disabilities Act; and
- 65 (8) Student or family Social Security numbers, only if needed by an institution of
66 higher education to comply with state or federal law.
- 67 3. No consent is needed in order for a public education agency or educational
68 institution to collect the following:
- 69 (1) Name, address, email address, and family contact information;
- 70 (2) State and national results of assessments approved by the general assembly
71 under subsection 2 of section 160.526;
- 72 (3) Courses taken and completed, and credits earned;
- 73 (4) Course grades earned and grade-point average;
- 74 (5) Date of birth, grade level, and expected graduation date;
- 75 (6) Degree, diploma, or credential attainment;
- 76 (7) Enrollment status;
- 77 (8) Attendance record and transfers;
- 78 (9) Discipline reports limited to objective information about disciplinary incidents;
- 79 (10) Juvenile delinquency or other criminal or correctional records if necessary to
80 meet the educational needs of the student or to ensure the safety of staff or students;
- 81 (11) Remediation data;
- 82 (12) Special education data, limited to data required by the federal Individuals with
83 Disabilities Education Act;
- 84 (13) Demographic data limited to race, economic status, disability status, and
85 English proficiency;

86 (14) Workforce information, as defined in this section, limited to information
87 relating to work-study programs in which participation was for academic credit;

88 (15) Student or family income data, limited to data required by law to determine
89 eligibility to participate in or receive financial assistance under a financial aid program;
90 and

91 (16) Information about extracurricular activities, limited to activities that are
92 school-sponsored or engaged in for academic credit.

93 4. Notwithstanding any other provision of law, no federal or state funds shall be
94 used on construction, enhancement, or expansion of any data system, as defined in this
95 section, that fails to comply with the privacy provisions of subsections 2 and 3 of this
96 section, or that is designed to track students beyond their K-12 careers, or to compile
97 student personal, nonacademic information beyond what is necessary for either
98 administrative functions directly related to a student's education or evaluation of academic
99 programs and student progress.

100 5. No student performance data shall be collected or disseminated in a manner that
101 violates the federal Fair Labor Standards Act of 1938.

102 6. No public education agency or educational institution shall pursue or accept any
103 grant that would require collecting or reporting any type of data in violation of sections
104 160.2510 to 160.2522.

 160.2512. 1. Public education agencies and educational institutions that maintain
2 a data system shall disclose publicly and conspicuously on the agency or educational
3 institution website the existence of such data system and the nature of the data system
4 including the following information:

5 (1) The legal authority for the establishment and existence of the data system;

6 (2) The principal purpose or purposes for which the information is intended to be
7 used;

8 (3) The categories of individuals on whom records are maintained;

9 (4) The categories of records maintained;

10 (5) Each expected disclosure of records, including the categories of recipients and
11 the purpose of such disclosure;

12 (6) The policies and practices of the public education agency or educational
13 institution regarding the storage, retrievability, access controls, retention, and disposal of
14 records;

15 (7) The title and business address of the official responsible for the data system and
16 the name and business address of any contractor or other outside party maintaining the
17 data system for or on behalf of the public education agency or educational institution;

(8) The procedure whereby parents, eligible students, or teachers can be notified at their request as to how to gain access to any record pertaining to the student or teacher and how content can be contested.

2. On request, parents and eligible students shall be provided a printed copy of their educational records that are held in any database and shall have the right to correct those educational records in a manner consistent with the requirements of state and federal law.

3. Public education agencies shall also provide annual electronic notification to the chairs of the senate education committee and the house elementary and secondary education committee of the existence of any data system. Public education agencies shall use only aggregate data in published reports.

160.2514. Notwithstanding any other provision of law, no school classroom, school district, state or national student assessment shall be adopted or administered in this state that collects any type of psychological data, including assessment of noncognitive skills or attribute, psychological resources, mindsets, learning strategies, effortful control, attitudes, dispositions, social skills, or other interpersonal or intrapersonal resources.

160.2516. No public education agency or educational institution shall administer any student survey, assessment, analysis, evaluation, or similar instrument that solicits information about the student or the student's family concerning the following:

(1) Political affiliations or beliefs;

(2) Mental or psychological problems, psychological resources, mindsets, learning strategies, effortful control, attributes, dispositions, social skills, attitudes, or intrapersonal resources;

(3) Sexual behavior or attitudes;

(4) Illegal, antisocial, self-incriminating, or demeaning behavior;

(5) Critical appraisals of another individual with whom a student has a close familial relationship;

(6) Legally recognized privileged relationships, including those with a lawyer, physician, or clergy person;

(7) Religious practices or beliefs;

(8) Personal or family gun ownership;

(9) Income or other income-related information except that required by law to determine eligibility to participate in or receive financial assistance under a program.

160.2518. 1. Any access to information collected under the provisions of sections 160.2510 to 160.2522 shall be restricted to an authorized representative or representatives of the public education agency or educational institution who requires such access to

4 perform work duties. No person may be designated as an authorized representative unless
5 such person is on the staff of the public education agency or educational institution and
6 under the direct control of the public education agency or educational institution.

7 2. Subject to the restrictions contained in sections 160.2510 to 160.2522, no
8 personally identifiable student data or teacher data shall be disclosed without the written
9 consent of the student's parent or guardian, or the student if he or she is emancipated, or
10 of the affected teacher.

11 3. The department of elementary and secondary education shall develop and
12 publish criteria for the approval of research-related data requests from state and local
13 governmental agencies, the legislature, academic researchers, and the public.

14 4. Notwithstanding any other provision of law, personally identifiable information
15 from an education report of a student or from teacher records shall not be released to a
16 party conducting studies for or on behalf of a public education agency or educational
17 institution without the written consent of a student's parent or guardian, or the student if
18 he or she is emancipated, or of the affected teacher, except to administer student financial
19 aid programs.

20 5. In conducting any audit or evaluation of an education program, or any
21 compliance or enforcement activity in connection with legal requirements relating to state
22 or district-supported education programs, any personally identifiable student or teacher
23 information, education records, and teacher records may be released only to an authorized
24 representative of a public education agency or educational institution. No party may be
25 designated as an authorized representative unless that party is on the staff and under the
26 direct control of the public education agency or educational institution.

27 6. Public agencies and educational institutions shall not disclose personally
28 identifiable information from education or teacher records without the informed written
29 consent of a parent or guardian of a student, or in the case of an emancipated minor the
30 informed written consent of a student, or the informed written consent of a teacher, to a
31 contractor, consultant, or other party to whom the public education agency or educational
32 institution has outsourced institutional services or functions unless the contractor,
33 consultant, or other party:

34 (1) Performs an institutional service or function for which the public education
35 agency or educational institution would otherwise use its own employees;

36 (2) Is under the direct control of the public education agency or educational
37 institution with respect to the use and maintenance of education records or teacher
38 records;

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

41 (4) Does not use the education records or teacher records for any purpose other
42 than those explicitly authorized in the contract;

43 (5) Does not disclose any personally identifiable information from education
44 records to any other party without the written consent of the parent, student, or teacher;
45 or unless required by statute or court order and the party provides notice of the disclosure
46 to the public education agency or educational institution that provided the information no
47 later than the time the information is disclosed, unless providing notice of the disclosure
48 is expressly prohibited by the statute or court order;

49 (6) Maintains industry standards for administrative, technical, and physical
50 safeguards to protect the security, confidentiality, and integrity of the personally
51 identifiable student or teacher data in its custody;

52 (7) Uses encryption technologies to protect data while in transmission or in its
53 custody from unauthorized disclosure using a technology or methodology specified by the
54 Secretary of the U.S. Department of Health and Human Services in guidance issued under
55 Section 13402(H)(2) of Public Law 111-5;

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

58 (9) Conducts a security audit annually and provides the results of that audit to each
59 public education agency or educational institution that provides education records or
60 teacher records;

61 (10) Provides the public education agency or educational institution with a breach-
62 remediation plan acceptable to the public education agency or educational institution
63 before initial receipt of education records or teacher records and makes results accessible
64 to the parents or guardians of the students;

65 (11) Reports all suspected and actual security breaches to the public education
66 agency or educational institution that provided education records or teacher records as
67 soon as possible but not later than forty-eight hours after a suspected or actual breach was
68 known or would have been known if exercising reasonable diligence, and also reports the
69 suspected or actual breach to the parent or guardian of a student or any other victim
70 connected to a suspected or actual security breach;

71 (12) Pays all costs and liabilities relating to the security breach or unauthorized
72 disclosure incurred by the public education agency or educational institution in the event
73 of a security breach or unauthorized disclosure of personally identifiable information,
74 including, but not limited to the costs of responding to inquiries about the security breach

75 or unauthorized disclosure, notifying subjects of personally identifiable information about
76 the breach, mitigating the effects of the breach for the subjects of the personally
77 identifiable information, and of investigating the cause or consequences of the security
78 breach or unauthorized disclosure; and

79 (13) Destroys or returns to the public education agency or educational institution
80 all personally identifiable information in its custody upon request and at the termination
81 of the contract.

160.2520. 1. In the event of a security breach or unauthorized disclosure of
2 personally identifiable student or teacher data, whether by a public education agency or
3 educational institution, or by a third party given access to education records or teacher
4 records under subsection 6 of section 160.2518, the public education agency or educational
5 institution shall:

6 (1) Immediately notify the subjects of the breach or disclosure;

7 (2) Report the breach or disclosure to the family policy compliance office of the U.S.
8 Department of Education; and

9 (3) Investigate the causes and consequences of the breach or disclosure.

10 2. Personally identifiable information from educational records or teacher records
11 shall not be disclosed to any party for commercial use including but not limited to
12 marketing products or services, compilation of lists for sale or rental, development of
13 products or services, or creation of individual, household, or group profiles.

14 3. Any cloud computing service provider performing services for a public education
15 agency or educational institution is prohibited from using information from education
16 records or teacher records for any secondary purposes that benefit the cloud computing
17 service provider or any third party, including but not limited to online behavioral
18 advertising, creating or correcting an individual or household profile primarily for the
19 cloud computing service provider's benefit, the sale of the data for any commercial
20 purpose, or any other similar commercial for-profit activity; provided, however, that a
21 cloud computing service provider may process or monitor student data solely to provide
22 such service to the public education agency or educational institution and to maintain the
23 integrity of such service.

24 4. Any cloud computing service provider that enters into an agreement to provide
25 cloud computing services to a public education agency or educational institution shall
26 certify in writing to the public education agency or educational institution that it will
27 comply with the terms and conditions set forth in sections 160.2510 to 160.2522 and that
28 the public education agency or educational institution maintains ownership of all student

29 and teacher data. Any student or teacher data stored by a cloud computing service
30 provider shall be stored within the boundaries of the United States.

31 5. No student data shall be used for predictive modeling for detecting behaviors,
32 beliefs, or value systems, or predicting or forecasting student outcomes.

33 6. There shall be no video monitoring of classrooms for any purpose, including for
34 teacher evaluation, without the approval of the district school board after public hearings
35 and the written consent of the teacher, all emancipated students, and the parents or
36 guardians of all other students in the classroom.

37 7. Personally identifiable information from education records or teacher records
38 shall not be disclosed to any noneducation government agency, including but not limited
39 to the Missouri department of labor, whether within or outside the state, or to any party
40 that intends to use or disclose the information or data for the purpose of workforce
41 development or economic planning. Data linkages or sharing of data with other states
42 without express permission of the individuals affected is prohibited.

43 8. Personally identifiable information from education records or teacher records
44 may not be disclosed to any government agency or other entity outside the state, except
45 disclosure may be made under the following circumstances:

46 (1) When a student has transferred to an educational institution out of state,
47 records may be disclosed to the out-of-state institution;

48 (2) When a student voluntarily participates in an out-of-state program for which
49 a data transfer is required for participation, records may be disclosed to the out-of-state
50 program; and

51 (3) When a student is classified as a migrant for federal reporting purposes.

52 9. No personally identifiable information from education records or teacher records
53 may be disclosed to any federal agency, including the U.S. Department of Education or the
54 U.S. Department of Labor or a representative, unless:

55 (1) Such disclosure is required by the U.S. Department of Education as a condition
56 of receiving a federal education grant;

57 (2) The U.S. Department of Education agrees in writing to use the information from
58 the education records or teacher records for the sole purpose of evaluating the program
59 or programs funded by a federal grant;

60 (3) The U.S. Department of Education agrees in writing that the information will
61 not be used for any research beyond that related to evaluation of the program or programs
62 funding by a federal grant, unless the parent or emancipated student or any teacher whose
63 information or data will be used for such evaluation affirmatively consents in writing to
64 such use;

65 (4) The U.S. Department of Education agrees in writing to destroy the information
66 or data upon completion of the evaluation of the program or programs for which the
67 information or data were compiled; and

68 (5) The grant or program in connection with which the information or data are
69 required is one explicitly authorized by federal statute or by federal rule promulgated
70 under the federal Administrative Procedure Act.

71 10. If the U.S. Department of Education demands personally identifiable student
72 information or teacher data without the written consent of the emancipated student, the
73 student's parents, or the teacher, the grant recipient shall provide written notification to
74 those emancipated students, parents, and teachers of the following:

75 (1) The grant recipient has been required to disclose the student's information or
76 teacher's data to the U.S. Department of Education;

77 (2) Neither the grant recipient or any other entity within the state of Missouri will
78 have control over use or further disclosure of that information or data; and

79 (3) The contact information, including the name, telephone number, and email
80 address of the U.S. Department of Education official who demands the disclosure.

81 11. Public agencies and educational institutions shall not disclose student or teacher
82 information to any assessment consortium of which the state is a member, or company with
83 which the state contracts for development or administration of any assessment unless:

84 (1) The information is transmitted in nonindividual record format;

85 (2) The information is limited to information directly related to the assessment,
86 such as a student's grade level and test scores; and

87 (3) No psychological information of any kind is included as part of the test scores.

88 12. An educational institution shall destroy and remove from the student database
89 all education records of a student within five years of the student's graduation from that
90 institution, provided that the institution may retain records showing dates of attendance,
91 diploma or degrees received, and contact information. If a student withdraws from an
92 education institution before graduating, the institution shall, within one year of the
93 student's withdrawal, destroy and remove from the database all education records of that
94 student except records showing dates of attendance. Destruction shall be compliant with
95 the NISTPS800-88 Standards.

 160.2522. 1. Each violation of any provision of sections 160.2510 to 160.2522 by an
2 organization or entity other than a public education agency or educational institution shall
3 be punishable by a civil penalty of a minimum of one thousand dollars; a second violation
4 by the same entity involving the education records and privacy of the same student shall
5 be punishable by a civil penalty of a minimum of five thousand dollars; and any

6 subsequent violation by the same entity involving the same student shall be punishable by
7 a civil penalty of a minimum of ten thousand dollars. Each violation involving a different
8 education record or a different individual student shall be considered a separate violation
9 for purposes of assessing civil penalties.

10 2. The attorney general shall have the authority to enforce compliance with sections
11 160.2510 to 160.2522.

Section B. Because immediate action is necessary to synchronize the requirements of this
2 act with the school calendar and state fiscal year, this act is deemed necessary for the immediate
3 preservation of the public health, welfare, peace, and safety, and is hereby declared to be an
4 emergency act within the meaning of the constitution, and this act shall be in full force and effect
5 on July 1, 2014, or upon its passage and approval, whichever occurs later.

✓