



128th MAINE LEGISLATURE

FIRST REGULAR SESSION-2017

Legislative Document

No. 1452

H.P. 1002

House of Representatives, April 18, 2017

An Act To Ensure Student Privacy in the Digital Age

Reference to the Committee on Education and Cultural Affairs suggested and ordered printed.

A handwritten signature in cursive script that reads "R B. Hunt".

ROBERT B. HUNT
Clerk

Presented by Representative SAMPSON of Alfred.
Cosponsored by Senator WOODSOME of York and
Representatives: FARNSWORTH of Portland, FULLER of Lewiston, GINZLER of Bridgton,
McCREA of Fort Fairfield, STEWART of Presque Isle, TURNER of Burlington, Senators:
BRAKEY of Androscoggin, MASON of Androscoggin.

1 **Be it enacted by the People of the State of Maine as follows:**

2 **Sec. 1. 20-A MRSA §952, sub-§1-A** is enacted to read:

3 **1-A. Acceptable use agreement.** "Acceptable use agreement" means an agreement
4 bound by certain restrictions and controls agreed to and signed by a 3rd party or an
5 employee or vendor of an organization.

6 **Sec. 2. 20-A MRSA §952, sub-§3,** as enacted by PL 2015, c. 256, §1, is amended
7 to read:

8 **3. Kindergarten to grade 12 school purposes.** "Kindergarten to grade 12 school
9 purposes" means purposes that take place at the direction of a school administrative unit,
10 a school that provides instruction to any grades from kindergarten to grade 12 or a teacher
11 at such a school or purposes that aid in the administration of school activities, including,
12 but not limited to, instruction in the classroom or at home, administrative activities,
13 preparation for postsecondary education or employment opportunities and collaboration
14 between students, school personnel or parents, or that are for the use and benefit of the
15 school. "Kindergarten to grade 12 school purposes" does not include research purposes.

16 **Sec. 3. 20-A MRSA §952, sub-§4,** as enacted by PL 2015, c. 256, §1, is amended
17 to read:

18 **4. Operator.** "Operator" means any entity other than the department, school
19 administrative unit or school to the extent that the entity:

20 A. Operates an Internet website, online service, online application or mobile
21 application with actual knowledge that the website, service or application is used for
22 kindergarten to grade 12 school purposes and was designed and marketed for
23 kindergarten to grade 12 school purposes to the extent that the operator is operating
24 in that capacity and collects, maintains or uses student personally identifiable
25 information in a digital or electronic format; and or

26 ~~B. Collects, maintains or uses student personally identifiable information in a digital~~
27 ~~or electronic format.~~

28 C. Provides services or applications to a researcher for research purposes that
29 transmit, store or process student personally identifiable information.

30 **Sec. 4. 20-A MRSA §952, sub-§§4-A to 4-E** are enacted to read:

31 **4-A. Protected student data.** "Protected student data" means student data that is
32 collected, stored, transmitted or processed for kindergarten to grade 12 school purposes.

33 **4-B. Research.** "Research" means a legitimate, clearly defined research project
34 using student data that is intended to improve the quality of instruction for students.

35 **4-C. Research agreement.** "Research agreement" means a legally binding
36 obligation, which requires protections of student privacy under this chapter, executed by a

1 researcher and the entity granting access to student personally identifiable information for
2 the purposes of research.

3 **4-D. Researcher.** "Researcher" means an individual, organization or entity,
4 including an institute of higher learning or government agency that conducts research.

5 **4-E. Safeguard.** "Safeguard" means an administrative, technical or physical control
6 to protect the security, integrity and confidentiality of student data.

7 **Sec. 5. 20-A MRSA §953, sub-§2, ¶A,** as enacted by PL 2015, c. 256, §1, is
8 amended to read:

9 A. Implement and maintain ~~reasonable security procedures and practices appropriate~~
10 ~~to the nature of the student data to protect that data from unauthorized access,~~
11 ~~destruction, use, modification and disclosure~~ safeguards equal to or greater than the
12 safeguards required under this chapter; and

13 **Sec. 6. 20-A MRSA §953, sub-§3, ¶A,** as enacted by PL 2015, c. 256, §1, is
14 amended to read:

15 A. Notwithstanding subsection 1, paragraph D, and in accordance with subsection 1,
16 paragraphs A, B and C, an operator may disclose student data under the following
17 circumstances:

18 (1) If another provision of federal or state law requires the operator to disclose
19 the student data and the operator complies with applicable requirements of
20 federal and state law in protecting and disclosing that information;

21 (2) For legitimate research purposes: under section 954; or

22 ~~(a) As required by state or federal law and subject to the restrictions under~~
23 ~~applicable state and federal law;~~ or

24 ~~(b) As allowed by state or federal law and under the direction of a school,~~
25 ~~school administrative unit or the department;~~ or

26 (3) To a state agency, school administrative unit or school for kindergarten to
27 grade 12 purposes, as permitted by state or federal law.

28 **Sec. 7. 20-A MRSA §953, sub-§4,** as enacted by PL 2015, c. 256, §1, is repealed.

29 **Sec. 8. 20-A MRSA §§954 to 959** are enacted to read:

30 **§954. Preservation of the security, confidentiality and integrity of student data**

31 **1. Safeguards required.** The department, each school administrative unit and all
32 state agencies shall develop, implement and maintain a comprehensive set of safeguards
33 regarding protected student data that the department, school administrative units and
34 relevant state agencies collect, store, transmit and process pursuant to rules adopted by
35 the state board under this subsection. In consultation with the Department of
36 Administrative and Financial Services, Office of Information Technology and other
37 agencies of the State as appropriate, the state board shall adopt rules to establish
38 requirements for safeguards, including:

- 1 A. Human resources practices, including background checks, disciplinary procedures
2 and application of access control principles, including limiting user access to only
3 information necessary for a particular use or purpose;
- 4 B. An acceptable use agreement;
- 5 C. Practices to minimize unauthorized access to student information and protected
6 student data;
- 7 D. Vendor management programs, including vendor management programs for
8 operators;
- 9 E. Employee security training and awareness programs;
- 10 F. Use of antivirus, monitoring, log review and management, configuration
11 management and vulnerability management practices;
- 12 G. Appropriate employment of firewalls, intrusion detection and prevention systems
13 and similar network security tools;
- 14 H. Development of incident management, breach response, audit and risk assessment
15 programs; and
- 16 I. Information asset management and disposal processes, including retention periods
17 for student data.

18 **2. Disclosure of student personally identifiable information to 3rd parties.**
19 Disclosure by the department, a school administrative unit or a state agency of student
20 personally identifiable information to any 3rd party, including the State Government or
21 Federal Government or an agent of the 3rd party, for kindergarten to grade 12 school
22 purposes, unless expressly exempted by law, requires the prior written consent of a parent
23 or guardian of the student or an eligible student. The organization granting access to the
24 information shall have a privacy policy requiring disclosure of the purpose and
25 identification of a recipient prior to the disclosure of student personally identifiable
26 information under this subsection.

27 **3. Disclosure without consent.** Student personally identifiable information may be
28 disclosed by the department, a school administrative unit or a state agency to a 3rd party
29 without consent:

- 30 A. When disclosure is otherwise required under federal law as a condition of federal
31 education funding administered by the department;
- 32 B. To develop, validate or administer statewide predictive tests;
- 33 C. To administer student aid programs;
- 34 D. When the information is governed and protected by privacy and security
35 protections established under the federal Health Information Portability and
36 Accountability Act of 1996, as amended, and accompanying federal regulations;
- 37 E. To ensure regulatory compliance;
- 38 F. To respond to or participate in a judicial process;

1 G. To a law enforcement agency or other governmental entity pursuant to a lawful
2 subpoena or as authorized or required by statute or rules of the court; or

3 H. In exigent circumstances to protect the safety of the student or others. The parent
4 or guardian of the student or the eligible student must be informed as soon as
5 reasonably possible after a disclosure under this paragraph.

6 The state board shall adopt rules to implement the provisions of this subsection and to
7 define additional circumstances allowing the disclosure of student personally identifiable
8 information without express written consent. Rules adopted under this subsection must
9 include consideration of the burden of obtaining consent, the educational benefit of such
10 disclosure, the period of retention of the information by a 3rd-party recipient and the
11 privacy practices and the safeguards to be implemented by a 3rd-party recipient.

12 **4. Student privacy officers.** The department, a school administrative unit and a
13 state agency that collects, stores, transmits and processes protected student data shall
14 designate an individual as the student privacy officer who is the responsible party for
15 implementing the requirements of this chapter for the officer's organization. The officer's
16 organization shall identify the officer in writing, and the officer is responsible to respond
17 to a parent or guardian of a protected student or an eligible student or to community
18 concerns regarding the privacy of protected student data. A student privacy officer's
19 contact information must be conspicuously posted on the organization's publicly
20 accessible website and must be included in privacy disclosures of the officer.

21 **5. Privacy policies and security practices.** The department, a school administrative
22 unit and a state agency subject to this chapter shall develop privacy policies and related
23 security practices that comprehensively implement the requirements of this chapter and
24 provide understandable and complete disclosures of the privacy policies and related
25 security practices to students and the students' parents or guardians or an eligible student
26 affected by the policies and practices.

27 **6. Research.** Student personally identifiable information may not be used for
28 research purposes without the prior written consent by a parent or guardian of the student
29 or by the eligible student. The department, a school administrative unit or a state agency
30 subject to this chapter shall provide to a parent or guardian of a student or an eligible
31 student an understandable, written description of the requested data and its use, a
32 maximum retention period after which secure destruction is assured and the consenting
33 parent's or guardian's or eligible student's right to revoke consent at any time. When
34 consent is granted under this subsection, research conducted with student personally
35 identifiable information is subject to the following requirements:

36 A. The researcher and any operator engaged in conjunction with the research shall
37 apply safeguards equal to or in excess of the requirements of this chapter and provide
38 3rd-party attestation by a reasonably qualified assessor of the researcher's or
39 operator's compliance with this chapter;

40 B. Student personally identifiable information may be used only by a researcher or
41 operator under the researcher's direction subject to a research agreement and the
42 information may not be transferred to other 3rd parties not bound by the research
43 agreement and expressly authorized by the provider of the data;

1 C. Research must be overseen by the department, a school administrative unit or a
2 state agency as allowed by state or federal law;

3 D. The researcher and an operator under the researcher's direction shall provide for
4 complete and unrecoverable deletion of student personally identifiable information
5 upon request by the consenting parent or guardian of the student or by the eligible
6 student within 5 days of written notice or a period specified within a research
7 agreement that may not exceed 30 days after substantial completion of the research;

8 E. The researcher shall designate an individual as a data steward who shall submit to
9 the jurisdiction of state law and be personally and severally liable for compliance
10 with the safeguard requirements of and rules adopted under this chapter; and

11 F. All research using student personally identifiable information must be reviewed
12 and approved by a nationally reputable institutional review board.

13 7. Waivers. A student who is not an eligible student may not waive any right or
14 obligation of any individual or entity subject to the requirements of this chapter regarding
15 that student's personally identifiable information.

16 **§955. Restrictions on collection and retention of protected student data**

17 1. Minimization; privacy assessment. The department, a school administrative unit
18 or a state agency is restricted in its collection of protected student data to the minimum
19 necessary to accomplish permissible kindergarten to grade 12 school purposes. Student
20 personally identifiable information may be collected only after completion of a privacy
21 assessment by the department, the school administrative unit or the state agency to
22 validate the necessity of the information and consideration of other reasonable means to
23 achieve the intended kindergarten to grade 12 school purposes, except that a privacy
24 assessment is not required for a federal or state legal or reporting obligation. A privacy
25 assessment under this subsection must be available to the public. The state board may
26 adopt rules identifying routine administrative cases where privacy assessments are not
27 required.

28 2. Sensitive data requiring consent. Except as provided in this chapter, the
29 department, a school administrative unit or a state agency may not collect, store, transmit
30 or process the following information from a student without the written consent of a
31 parent or guardian of a student or an eligible student unless otherwise required or
32 authorized by statute or rule:

33 A. DNA, fingerprints or retina or iris pattern information or any information about
34 the psychological characteristics of a student;

35 B. A student's or student's family's religious affiliation, beliefs or practices;

36 C. A student's or student's family's political affiliation, beliefs or practices;

37 D. A student's or student's family member's sexual orientation or beliefs about sexual
38 orientation; or

39 E. A student's or student's family's gun ownership or usage.

1 **3. Monitoring of student electronic devices.** A school administrative unit may
2 monitor the use of students' electronic devices only to the extent necessary for efficient
3 operation of school infrastructure, for the physical safety of the school or to ensure that
4 the use is consistent with educational purposes during school hours. The state board shall
5 adopt rules to implement the provisions of this subsection.

6 **§956. Right to inspect and correct student data**

7 **1. Right to inspect.** The department, a school administrative unit or a school may
8 not deny or prevent a parent or guardian of a student or an eligible student who is or has
9 been in attendance at a school the right to inspect and review the student personally
10 identifiable information comprising the education records of the student or eligible
11 student. If any material or document in the education records of a student includes student
12 personally identifiable information of more than one student, the parent or guardian of the
13 subject student or a subject eligible student has the right to inspect and review only the
14 part of the material or document that relates to the subject student or to be informed of the
15 specific information contained in that part of the material that relates to the subject
16 student. The department, the school administrative unit, the school or other affected
17 agency shall establish appropriate procedures for the granting of a request by a parent or
18 guardian of a subject student or a subject eligible student for access to the records of that
19 student within a reasonable period of time that may not exceed 45 days after the request
20 has been made.

21 **2. Right to make corrections.** The department, a school administrative unit or a
22 school may not deny or prevent a parent or guardian of a student or an eligible student the
23 opportunity for a hearing to challenge the content of the student's personally identifiable
24 information to ensure that the student's personally identifiable information is not
25 inaccurate, misleading or otherwise in violation of the privacy rights of the student, to
26 provide an opportunity to correct or delete inaccurate, misleading or otherwise
27 inappropriate information or to insert into the student's personally identifiable
28 information a written explanation of the parent or guardian of the student or the eligible
29 student regarding the content of the student's personally identifiable information.

30 **§957. State education privacy officer**

31 **1. State education privacy officer; established.** The position of state education
32 privacy officer is established within the department. The state board shall hire the state
33 education privacy officer, who serves at the direction of the state board.

34 **2. Duties.** Under the supervision of the state board, the state education privacy
35 officer is responsible for implementation and oversight of this chapter, including the
36 following duties:

37 A. Representing the interests of students and parents and guardians of students in
38 preserving student privacy in the State;

39 B. Advising the state board on policy and rules necessary to effectively protect the
40 privacy of protected student data consistent with this chapter;

1 C. With the approval of the state board, issuing guidance regarding privacy
2 principles and best practices to be followed by the department, school administrative
3 units and other agencies subject to this chapter, including the content of privacy
4 disclosures and practices such as disclosure, content and retention of databases of
5 protected student data;

6 D. Assessing and monitoring the effectiveness of the implementation of safeguards
7 established pursuant to section 954; and

8 E. Reporting at least biennially on student education privacy to the state board, the
9 Legislature and the Governor.

10 **3. Public complaints.** The state education privacy officer may investigate
11 complaints affecting the privacy of students and, when appropriate, make
12 recommendations to the state board concerning these complaints.

13 **§958. Construction; penalties**

14 **1. Construction.** The following provisions govern the application and construction
15 of this chapter.

16 A. This chapter may not be construed to limit the authority of a law enforcement
17 agency to obtain any content or student data from an operator as authorized by law or
18 pursuant to an order of a court of competent jurisdiction.

19 B. This chapter does not apply to general audience Internet websites, general
20 audience online services, general audience online applications or general audience
21 mobile applications even if user names or passwords created for an operator's site,
22 service or application are used to access those general audience sites, services or
23 applications.

24 C. This chapter may not be construed to restrict Internet service providers from
25 providing Internet connectivity to schools or students and their families.

26 D. This chapter may not be construed to prohibit an operator from marketing
27 educational products directly to parents so long as the marketing does not result from
28 the use of protected student data obtained without parental consent by the operator
29 through the provision of services covered under this chapter.

30 E. This chapter may not be construed to impose a duty upon a provider of an
31 electronic means of purchasing or downloading software or applications to review or
32 enforce compliance with this chapter with respect to those applications or software.

33 F. This chapter may not be construed to impose a duty upon a provider of an
34 interactive computer service, as defined in 47 United States Code, Section 230, to
35 review or enforce compliance with this chapter by 3rd-party content providers.

36 G. This chapter may not be construed to impede the ability of a student or a student's
37 parent or guardian or an eligible student to download, transfer or otherwise save or
38 maintain protected student data or documents belonging to the student.

39 H. Nothing in this chapter prevents the State or a school administrative unit or an
40 employee of the State or a school administrative unit from recommending, directly or

1 indirectly, any educational materials, online content, services or products to a student
2 or the student's family if the State or a school administrative unit determines that such
3 a product or service will benefit the student and the State or the school administrative
4 unit does not receive compensation for developing, enabling or communicating such
5 recommendations.

6 I. Nothing in this chapter authorizes the dissemination of information in violation of
7 section 6001.

8 **2. Civil penalty; disqualification.** A violation of this chapter by a recipient of
9 protected student data, including any operator, contractor, consultant or other party that is
10 subject to the provisions of this chapter, is subject to a fine or civil penalty of up to
11 \$5,000 and may be permanently disqualified by the department or a school administrative
12 unit or a school from access to education records. Each violation involving a different
13 individual student is considered a separate violation under this subsection.

14 **3. Enforcement by Attorney General.** The Attorney General has the authority to
15 enforce compliance with this chapter.

16 **4. Private right of action.** A parent or guardian of a student or an eligible student
17 has a private right of action against a 3rd-party recipient of student personally identifiable
18 information or protected student data that does not comply with the safeguards or other
19 requirements of this chapter. In addition to the civil penalty under subsection 2, a private
20 right of action under this subsection includes the right to treble damages, consequential
21 and punitive damages and reasonable attorney's fees. This subsection does not create a
22 private right of action against a data steward in section 954, subsection 6, paragraph E or
23 the department, a school administrative unit or other state agency except when a school
24 administrative unit or school within a school administrative unit fails to provide timely
25 access to protected student data or the opportunity for a parent, guardian or eligible
26 student to correct the data under section 956.

27 **§959. Rules**

28 The state board may adopt rules to carry out the provisions of this chapter. Rules
29 adopted pursuant to this section are major substantive rules as defined in Title 5, chapter
30 375, subchapter 2-A.

31 **Sec. 9. Rulemaking.** By October 31, 2018, the State Board of Education
32 established by the Maine Revised Statutes, Title 5, section 12004-C, subsection 1 shall
33 adopt rules necessary to implement this Act on its effective date. Rules adopted pursuant
34 to this section are routine technical rules as defined in Title 5, chapter 375, subchapter
35 2-A.

36 **Sec. 10. Effective date.** Those sections of this Act that amend the Maine Revised
37 Statutes, Title 20-A, sections 952 and 953 and that enact Title 20-A, sections 954 to 959
38 take effect July 1, 2019 and apply beginning with the 2018-2019 school year.

1 **SUMMARY**

2 This bill:

3 1. Establishes data privacy practices for the Department of Education, school
4 administrative units, schools, other agencies and 3rd parties handling protected student
5 data;

6 2. Subject to rule-making authority granted to the State Board of Education, requires
7 administrative, physical and technical safeguards to be implemented to protect the
8 privacy and integrity of protected student data;

9 3. Requires written consent by a parent or guardian of a student or by a student 18
10 years of age or older to share the student's personally identifiable information, with
11 protections when no consent is required;

12 4. Subjects research using student personally identifiable information to student
13 privacy protections;

14 5. Provides requirements for the minimization of and prohibitions on, the collection
15 of certain information without consent;

16 6. Establishes the right of a parent or guardian of a student or a student 18 years of
17 age or older to inspect the student's personally identifiable information and make
18 corrections for inaccuracies or misleading data;

19 7. Ensures the effectiveness of privacy protections of students by establishing the
20 position of a state education privacy officer within the Department of Education who is
21 responsible to the State Board of Education;

22 8. Establishes a private right of action including civil penalties and damages against
23 3rd parties for failure to adequately protect student personally identifiable information or
24 protected student data against the department, school administrative units or schools,
25 except under specific circumstances; and

26 9. Requires the provisions of this Act be implemented by routine technical rules prior
27 to October 31, 2018 and any rules adopted after the effective date of this Act on July 1,
28 2019 be major substantive rules.