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.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. Human resources practices, including background checks, disciplinary procedures and application of access control principles, including limiting user access to only information necessary for a particular use or purpose;

B. An acceptable use agreement;

C. Practices to minimize unauthorized access to student information and protected student data;

D. Vendor management programs, including vendor management programs for operators;

E. Employee security training and awareness programs;

F. Use of antivirus, monitoring, log review and management, configuration management and vulnerability management practices;

G. Appropriate employment of firewalls, intrusion detection and prevention systems and similar network security tools;

H. Development of incident management, breech response, audit and risk assessment programs; and

I. Information asset management and disposal processes, including retention periods for student data.

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

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

A. When disclosure is otherwise required under federal law as a condition of federal education funding administered by the department;

B. To develop, validate or administer statewide predictive tests;

C. To administer student aid programs;

D. When the information is governed and protected by privacy and security protections established under the federal Health Information Portability and Accountability Act of 1996, as amended, and accompanying federal regulations;

E. To ensure regulatory compliance;

F. To respond to or participate in a judicial process;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§956. Right to inspect and correct student data

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

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

§957. State education privacy officer

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

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

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

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

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

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

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

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

§958. Construction; penalties

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§959. Rules

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

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

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

SUMMARY

This bill:

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

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

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

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

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

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

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

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

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