

MAINE STATE LEGISLATURE

The following document is provided by the
LAW AND LEGISLATIVE DIGITAL LIBRARY
at the Maine State Law and Legislative Reference Library
<http://legislature.maine.gov/lawlib>



Reproduced from electronic originals
(may include minor formatting differences from printed original)



127th MAINE LEGISLATURE

FIRST REGULAR SESSION-2015

Legislative Document

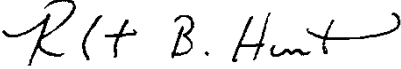
No. 1252

H.P. 852

House of Representatives, April 7, 2015

An Act To Protect Student Data

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


ROBERT B. HUNT
Clerk

Presented by Representative MOONEN of Portland.
Cosponsored by Representative: GUERIN of Glenburn.

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

2 **Sec. 1. 20-A MRSA §6006** is enacted to read:

3 **§6006. Student electronic data**

4 **1. Definitions.** As used in this section, unless the context otherwise indicates, the
5 following terms have the following meanings.

6 A. "Aggregate data" means student-related data collected and reported by an
7 educational institution at the group, cohort or institutional level that contain no
8 personally identifying student data.

9 B. "Educational institution" means a school administrative unit or private or public
10 elementary or secondary school under this Part or Part 2, including an employee or
11 agent of the unit or school acting as representative or on behalf of the unit or school.

12 C. "Personally identifying student data" means student data that include:

13 (1) The name of a student or a parent, legal guardian or family member of a
14 student;

15 (2) The address of a student or a parent, legal guardian or family member of a
16 student;

17 (3) A student's date of birth, place of birth, social security number, telephone
18 number, credit card account number, insurance account number, financial
19 services account number, e-mail address, social media address or password or
20 any other electronic address; and

21 (4) Any information that, alone or in combination, is linked or linkable to a
22 specific student that would allow a 3rd party to identify the student with
23 reasonable certainty.

24 D. "Provider" means a person who sells, leases or provides to or operates or
25 maintains for an educational institution a student information system.

26 E. "Student data" means data about a student that are collected and stored by an
27 educational institution and included in a student's educational record.

28 F. "Student information system" means a software application that allows an
29 educational institution to input, maintain and manage student data on a computer or
30 computer system.

31 G. "System opt-in agreement" means a verifiable written or electronically generated
32 agreement by which access is granted to analyze, interact with, share or transfer
33 specific personally identifying student data.

34 **2. Student information system.** A contract or agreement between an educational
35 institution and a provider:

36 A. Must expressly authorize and require the secure storage and transmission of all
37 student data;

1 B. May authorize the provider to access, analyze, interact with, share or transfer
2 aggregate data transferred or stored in the student information system; and

3 C. Must expressly prohibit the provider from accessing, analyzing, interacting with,
4 sharing or transferring any personally identifying student data transferred or stored in
5 the student information system unless:

6 (1) The provider receives a valid system opt-in agreement under subsection 3 for
7 the personally identifying student data; or

8 (2) At the request of the educational institution, the provider de-identifies and
9 aggregates personally identifying student data for the sole purpose of enabling
10 the educational institution to comply with federal, state or local reporting
11 requirements.

12 **3. System opt-in agreement.** A system opt-in agreement must be signed by a
13 student and, if the student is less than 18 years of age, a parent or legal guardian of the
14 student. A student or parent or legal guardian of the student is not required to sign a
15 system opt-in agreement. A system opt-in agreement may be revoked at any time upon
16 written notice by the student or a parent or legal guardian of the student. An educational
17 benefit may not be withheld from or punitive measure taken against a student or parent,
18 legal guardian or family member of the student based in whole or in part upon a decision
19 not to sign or to revoke a system opt-in agreement. A provider may not share, sell or
20 otherwise transfer personally identifying student data obtained from a system opt-in
21 agreement except as provided in subsection 4. A system opt-in agreement may not grant
22 general access to personally identifying student data. A valid system opt-in agreement
23 must specify:

24 A. The name of the provider to whom access is being granted;

25 B. The precise subset of personally identifying student data in the student
26 information system, such as attendance records or disciplinary records, to which the
27 provider is being granted access;

28 C. The purpose for the access; and

29 D. Any information required by subsection 4.

30 **4. Sharing or transferring personally identifying student data with or to a 3rd**
31 **party.** A provider may share with or transfer or otherwise disseminate to a 3rd party
32 personally identifying student data if:

33 A. The 3rd party is identified in the system opt-in agreement of the student under
34 subsection 3;

35 B. The purpose of the sharing or transfer of the personally identifying student data is
36 to benefit the operational, administrative or educational functions of the educational
37 institution and that benefit is specified in the system opt-in agreement of the student
38 under subsection 3;

39 C. The system opt-in agreement under subsection 3 specifies the subset of personally
40 identifying student data, such as attendance records or disciplinary records, to be
41 shared or transferred; and

1 D. Prior to sharing or transferring the personally identifying student data, the
2 provider notifies the 3rd party in writing that the 3rd party may not share the data
3 with or transfer or otherwise disseminate the data to another person not authorized
4 under this section.

5 A person who directly or indirectly receives personally identifying student data under this
6 subsection may not share the data with or transfer or otherwise disseminate the data to
7 another person not authorized under this section.

8 **5. Educational institution employees.** An educational institution may authorize in
9 writing an employee of the educational institution to access personally identifying student
10 data on a student information system if the employee is trained regarding the provisions
11 of this section and the access is limited to the extent required by the employee's
12 professional duties. An employee under this subsection may not share, transfer or
13 otherwise disseminate personally identifying student data unless specifically authorized
14 under this section.

15 **6. Parent or legal guardian of student.** Upon written request, a parent or legal
16 guardian of a student or a student who is 18 years of age or older may review the student's
17 personally identifying student data that are stored on a student information system and
18 may request a correction to or seek removal of inaccurate data.

19 **7. Removal of personally identifying student data.** Except as otherwise provided
20 by law or if retention of personally identifying student data is required pursuant to a
21 disciplinary, administrative or judicial action or proceeding, upon a student's graduation,
22 withdrawal or expulsion from an educational institution, the educational institution and
23 any employee, provider or 3rd party in possession of any of the student's personally
24 identifying student data shall delete or otherwise destroy the data. Within 30 days of the
25 student's graduation, withdrawal or expulsion from the educational institution, the
26 educational institution shall notify any employee, provider or 3rd party in possession of
27 the student's personally identifying student data of the provisions of this subsection.

28 **8. Limitations on use.** Evidence or information obtained or collected in violation of
29 this section is not admissible as evidence in any disciplinary, administrative, civil or
30 criminal trial, proceeding or hearing.

31 **9. Penalty.** An educational institution that violates this section is subject to the
32 provisions of section 6801-A.

33 **Sec. 2. 20-A MRSA c. 231** is enacted to read:

34 **CHAPTER 231**
35 **ELECTRONIC DEVICES**

36 **§6991. Definitions**

37 As used in this chapter, unless the context otherwise indicates, the following terms
38 have the following meanings.

1 **1. Device opt-in agreement.** "Device opt-in agreement" means a verifiable written
2 or electronically generated agreement by which access is granted to analyze, interact
3 with, share or transfer specific personally identifying student data stored on a student
4 electronic device.

5 **2. Educational institution.** "Educational institution" means a school administrative
6 unit or private or public elementary or secondary school under this part or Part 2,
7 including an employee or agent of the unit or school acting as representative or on behalf
8 of the unit or school.

9 **3. Electronic device.** "Electronic device" has the same meaning as in Title 16,
10 section 647, subsection 3.

11 **4. Personal electronic device.** "Personal electronic device" means an electronic
12 device that was not provided by an educational institution and is owned, leased or
13 possessed by a student.

14 **5. Personally identifying student data.** "Personally identifying student data"
15 means student data that include:

16 A. The name of a student or a parent, legal guardian or family member of a student;

17 B. The address of a student or a parent, legal guardian or family member of a
18 student;

19 C. A student's date of birth, place of birth, social security number, telephone number,
20 credit card account number, insurance account number, financial services account
21 number, e-mail address, social media address or password or any other electronic
22 address; and

23 D. Any information that, alone or in combination, is linked or linkable to a specific
24 student that would allow a 3rd party to identify the student with reasonable certainty.

25 **6. School-authorized electronic device.** "School-authorized electronic device"
26 means an electronic device that an educational institution or a 3rd party approved by the
27 educational institution provides to a student for overnight or at-home use.

28 **7. Student data.** "Student data" means data on a school-authorized electronic device
29 or a personal electronic device, including browser, keystroke and location histories.

30 **§6992. School-authorized electronic devices**

31 **1. School-authorized electronic devices.** An educational institution, employee of
32 an educational institution or 3rd party may not directly or remotely access a school-
33 authorized electronic device or data stored on a school-authorized electronic device or
34 share, transfer or otherwise disseminate data stored on a school-authorized electronic
35 device, except pursuant to the provisions of this section.

36 **2. Access to a school-authorized electronic device.** As specified in this subsection,
37 an educational institution, employee of the educational institution, law enforcement
38 official or 3rd party may access a school-authorized electronic device owned by the
39 educational institution to analyze, interact with, share or transfer student data if:

1 A. For the educational institution, employee of the educational institution or 3rd
2 party authorized by the educational institution:

3 (1) The data are not personally identifying student data;

4 (2) The educational institution, employee of the educational institution or 3rd
5 party obtains a device opt-in agreement under subsection 7 authorizing the
6 specific scope of the access; or

7 (3) Access is necessary to update or upgrade the device's software and access is
8 limited to that purpose;

9 B. For the educational institution or employee of the educational institution, the
10 educational institution or employee has reasonable suspicion that the student has
11 violated or is violating the educational institution's policy and that the device contains
12 evidence of the suspected violation, subject to the following:

13 (1) Prior to searching the device, the educational institution or employee
14 documents the reasonable suspicion and notifies the student and, if the student is
15 less than 18 years of age, a parent or legal guardian of the student of the
16 suspected violation and the specific data to be searched for evidence of the
17 violation;

18 (2) The search is strictly limited to the data listed in subparagraph (1); and

19 (3) If the violation involves illegal conduct, a judicial warrant is obtained
20 pursuant to paragraph C prior to the search even if the device may also have
21 evidence of a related or unrelated violation of the educational institution's policy;

22 C. For the educational institution, employee of the educational institution or law
23 enforcement official, the educational institution, employee or law enforcement
24 official reasonably suspects the student has engaged or is engaging in illegal conduct
25 and reasonably suspects that data on the device contain evidence of the suspected
26 illegal conduct and has obtained a judicial warrant to search the device prior to the
27 search. A 3rd party other than a law enforcement official may not access a student
28 electronic device pursuant to this paragraph; or

29 D. For the educational institution, employee of the educational institution, law
30 enforcement official or 3rd party, access by the educational institution, employee, law
31 enforcement official or 3rd party is necessary in response to an immediate threat to
32 life or safety and access is limited to that purpose. Within 72 hours of accessing a
33 device under this paragraph, the educational institution, employee of the educational
34 institution, law enforcement official or 3rd party shall provide to the student whose
35 device was accessed, to a parent or legal guardian of the student if the student is less
36 than 18 years of age and to the educational institution if the access was performed by
37 an employee of the educational institution, law enforcement official or 3rd party a
38 written explanation of the precise threat that prompted the access and the specific
39 data that were accessed.

40 **3. Tracking location.** If a school-authorized electronic device is equipped with
41 location tracking technology, either to track the location in real time or a historical
42 location, an educational institution, employee of an educational institution or law
43 enforcement official may use the tracking technology to track the device if:

1 A. The use is ordered pursuant to a judicial warrant. A 3rd party other than a law
2 enforcement official may not access a student electronic device pursuant to this
3 paragraph;

4 B. The student or a parent or legal guardian of the student to whom the device was
5 provided has notified the educational institution, employee of an educational
6 institution or a law enforcement official in writing that the device was lost or stolen;
7 or

8 C. Tracking the device is necessary in response to an immediate threat to life or
9 safety and access is limited to that purpose. Within 72 hours of using tracking
10 technology of a device under this paragraph, the educational institution, employee of
11 an educational institution or 3rd party or a law enforcement official shall provide to
12 the student whose device was tracked, to a parent or legal guardian of the student if
13 the student is less than 18 years of age and to the educational institution if the
14 tracking was performed by an employee of an educational institution or a law
15 enforcement official a written explanation of the precise threat that prompted the
16 tracking and the specific details of the tracking.

17 **4. Audio or video functions.** An educational institution, employee of the
18 educational institution, law enforcement official or 3rd party may activate or access any
19 audio or video receiving, transmitting or recording functions on a school-authorized
20 electronic device if:

21 A. The student to whom the device was provided initiates the video or audio function
22 for an educational purpose and activation or access by the educational institution,
23 employee of the educational institution, law enforcement official or 3rd party is
24 limited to that purpose;

25 B. The activation or access is ordered by a judicial warrant. A 3rd party other than a
26 law enforcement official may not activate or access any audio or video receiving,
27 transmitting or recording functions of a student electronic device pursuant to this
28 paragraph; or

29 C. Activating or accessing the audio or video function of the device is necessary in
30 response to an immediate threat to life or safety and access is limited to that purpose.
31 Within 72 hours of activating or accessing the audio or video function of a device
32 under this paragraph, the educational institution, employee of the educational
33 institution, law enforcement official or 3rd party shall provide to the student whose
34 device's audio or video function was activated or accessed, to a parent or legal
35 guardian of the student if the student is less than 18 years of age and to the
36 educational institution if the activation or access was performed by an employee of
37 the educational institution or a law enforcement official a written explanation of the
38 precise threat that prompted the activation or access and the specific details of the
39 activation or access.

40 **5. Employee training.** An employee of an educational institution may not
41 supervise, direct or participate in an educational program using a school-authorized
42 electronic device without receiving adequate training on the provisions of this section.

1 **6. Sharing, transferring or dissemination of personally identifying student data.**

2 Personally identifying student data obtained from a school-authorized electronic device
3 may not be shared with or transferred or disseminated to an employee of an educational
4 institution who has not satisfied the requirements of subsection 5.

5 **7. Device opt-in agreement.** A device opt-in agreement must be signed by the
6 student to whom a school-authorized electronic device is provided and, if the student is
7 less than 18 years of age, a parent or legal guardian of the student. A student or parent or
8 legal guardian of the student is not required to sign a device opt-in agreement. A device
9 opt-in agreement may be revoked at any time upon written notice by the student or a
10 parent or legal guardian of the student. An educational benefit may not be withheld from
11 or punitive measure taken against a student or parent, legal guardian or family member of
12 the student based in whole or in part upon a decision not to sign or to revoke a device opt-
13 in agreement. A device opt-in agreement may not grant general access to personally
14 identifying student data and may not grant to a 3rd party authority to collect all the
15 personally identifying student data that are generated or used in connection with a
16 specific program or application on the device. A device opt-in agreement may not allow
17 an educational institution, an employee of an educational institution or a 3rd party to
18 share, sell or otherwise transfer personally identifying student data to a 3rd party. A valid
19 device opt-in agreement must specify:

20 A. The name of the employee of the educational institution or 3rd party to whom
21 access is being granted;

22 B. The precise subset of personally identifying data to which the person in paragraph
23 A is being granted access; and

24 C. The purpose for the access.

25 **8. School-authorized program.** A school-authorized program requiring use of a
26 school-authorized electronic device may not condition a student's participation in the
27 program upon execution of a device opt-in agreement or authorization by the student or
28 the student's parent or legal guardian to allow access to the student's personally
29 identifying student data on a school-authorized electronic device.

30 **9. Return of device.** Upon return of a school-authorized electronic device to an
31 educational institution from a student, the educational institution shall fully erase all data
32 stored on the device and return the device to its default factory settings.

33 **10. Limitations on use.** Evidence or information obtained or collected in violation
34 of this section is not admissible as evidence in any disciplinary, administrative, civil or
35 criminal trial, proceeding or hearing.

36 **11. Penalty.** An educational institution that violates this section is subject to the
37 provisions of section 6801-A.

38 **§6993. Personal electronic devices**

39 **1. Personal electronic devices.** An educational institution, at its discretion, may
40 limit or prohibit a student from carrying or using a personal electronic device while on
41 the property of the educational institution. An educational institution, employee of an

1 educational institution or 3rd party may not directly or remotely access a personal
2 electronic device or data stored on a personal electronic device or share, transfer or
3 otherwise disseminate data stored on a personal electronic device, except pursuant to the
4 provisions of this section.

5 **2. Access to a personal electronic device.** As specified in this subsection, an
6 educational institution, employee of the educational institution, law enforcement official
7 or 3rd party may not access any data or other content input into or stored on a personal
8 electronic device of a student of the educational institution, even if the device has been
9 carried or used in violation of the policy of the educational institution, unless:

10 A. For the educational institution or employee of the educational institution, the
11 educational institution or employee has reasonable suspicion that the student has
12 violated or is violating the educational institution's policy and the device contains
13 evidence of the suspected violation, subject to the following:

14 (1) Prior to searching the device, the educational institution or employee
15 documents the reasonable suspicion and notifies the student and, if the student is
16 less than 18 years of age, a parent or legal guardian of the student of the
17 suspected violation and the specific data to be searched for evidence of the
18 violation;

19 (2) The search is strictly limited to the data listed in subparagraph (1); and

20 (3) If the violation involves illegal conduct, a judicial warrant is obtained
21 pursuant to paragraph B prior to the search even if the device may also have
22 evidence of a related or unrelated violation of the educational institution's policy;

23 B. For the educational institution, employee of the educational institution or law
24 enforcement official, the educational institution, employee or law enforcement
25 official reasonably suspects the student has engaged or is engaging in illegal conduct,
26 reasonably suspects that data on the device contain evidence of the suspected illegal
27 conduct and has obtained a judicial warrant to search the device prior to the search. A
28 3rd party other than a law enforcement official may not access a student electronic
29 device pursuant to this paragraph; or

30 C. For the educational institution, employee of the educational institution, law
31 enforcement official or 3rd party, access by the educational institution, employee, law
32 enforcement official or 3rd party is necessary in response to an immediate threat to
33 life or safety and access is limited to that purpose. Within 72 hours of accessing a
34 device under this paragraph, the educational institution, employee, law enforcement
35 official or 3rd party shall provide to the student whose device was accessed, to a
36 parent or legal guardian of the student if the student is less than 18 years of age and to
37 the educational institution if the access was performed by an employee of the
38 educational institution, law enforcement official or 3rd party a written explanation of
39 the precise threat that prompted the access and the specific data that were accessed.

40 **3. Sharing, transferring or dissemination of personally identifying student data.**
41 Personally identifying student data obtained from a personal electronic device may not be
42 shared with or transferred or disseminated to a 3rd party without the express written

1 consent of the student and, if the student is less than 18 years of age, a parent or legal
2 guardian of the student.

3 **4. Limitations on use.** Evidence or information obtained or collected in violation of
4 this section is not admissible as evidence in any disciplinary, administrative, civil or
5 criminal trial, proceeding or hearing.

6 **5. Penalty.** An educational institution that violates this section is subject to the
7 provisions of section 6801-A.

8 **SUMMARY**

9 This bill establishes restrictions and protocols on the access and use of personally
10 identifying student data by public and private elementary and secondary schools in
11 software applications used to input, store and manage student data and on school-
12 authorized electronic devices provided to students for overnight or at-home use. This bill
13 also establishes restrictions and protocols for public and private elementary and
14 secondary schools regarding allowable limitations on students' possession and use of and
15 the schools' authority to access data on students' personal electronic devices.