

2017 -- H 5682

=====
LC001954
=====

STATE OF RHODE ISLAND

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2017

—————
A N A C T

RELATING TO EDUCATION -- PROTECTING STUDENT PRIVACY ON SCHOOL-
OWNED TECHNOLOGY

Introduced By: Representatives Kennedy, O`Grady, Casey, Johnston, and Kazarian

Date Introduced: March 01, 2017

Referred To: House Health, Education & Welfare

It is enacted by the General Assembly as follows:

1 SECTION 1. Title 16 of the General Laws entitled "EDUCATION" is hereby amended
2 by adding thereto the following chapter:

3 CHAPTER 107

4 STUDENT PRIVACY IN TAKE-HOME TECHNOLOGY PROGRAMS

5 **16-107-1. Definitions.**

6 For the purposes of this chapter:

7 (1) "Educational institution" or "school" means a private or public institution that offers
8 participants, students, or trainees an organized course of study or training that is academic, trade-
9 oriented or preparatory for gainful employment in a recognized occupation and shall include any
10 person acting as an agent of the institution.

11 (2) "Device" means any computer, including laptop or tablet computers, or other
12 electronic device owned or maintained by the educational institution and provided to a student
13 pursuant to a take-home technology program.

14 (3) "Internet filtering measures" means the use of a specific technology or program to
15 block or filter access to websites on the Internet.

16 (4) "Location tracking" means a global positioning service or other mapping, locational,
17 or directional information service, used to determine the location of the device in real time or
18 historically.

1 (5) "Remote access" means the ability to access a computer from a remote location. This
2 includes the ability to view a computer's network, desktop or files from an external location or
3 server, as well as the ability to open, modify, or delete programs.

4 (6) "Take-home technology program" means any program wherein a device is provided
5 to a student for overnight or at-home use.

6 (7) "Student" means any student, participant, or trainee, whether full-time or part-time, in
7 an organized course of study at an educational institution.

8 **16-107-2. Optional participation in take-home technology programs.**

9 (a) No educational institution shall compel, coerce, or require a student to participate in a
10 take-home technology program.

11 (b) No student shall be permitted to participate in a take-home technology program
12 without the written consent of the student's parent or guardian, including the signing of an opt-in
13 agreement.

14 (c) A valid opt-in agreement shall identify, with specificity:

15 (1) The precise subset of data on the device to which access is being granted;

16 (2) The name of the school employee(s) or third party to whom the authority to access the
17 data on the device is being granted;

18 (3) The name of any third party to whom data is being sold, shared, or otherwise
19 transferred; and

20 (4) The purpose(s) for which the school employee(s) or third party is being granted
21 access to the device or for which data is being sold, shared, or otherwise transferred.

22 (d) An opt-in agreement shall not be valid if it actually or effectively grants a third party:

23 (1) General authority to access a student's device; or

24 (2) The authority to collect all personally-identifiable student data that is generated by
25 and/or used in connection with a specific program or application.

26 (e) No third party or school employee who receives personally identifiable information
27 from a device pursuant to an opt-in agreement may share, sell or otherwise transfer such data to
28 another third party.

29 (f) An opt-in agreement may be revoked at any time, upon written notice to an
30 educational institution, by a student or their parent or guardian. Within fourteen (14) days of such
31 a revocation, notice to any affected third parties shall be made by the educational institution.

32 (g) No device or other educational benefit may be withheld from, or punitive measure
33 taken against, a student or their parent or legal guardian:

34 (1) Based in whole or in part upon a decision not to sign, or to revoke, an opt-in

1 agreement; or

2 (2) Based in whole or in part upon a student's refusal to open, close, or maintain an e-mail
3 or other electronic communications or social media account with a specific service provider.

4 (h) Where a take-home technology program is offered at an educational institution, any
5 attempt by the educational institution or a third party to condition the offer, provision or receipt of
6 a device upon a student's or their parent's or legal guardian's agreement to provide or permit the
7 sharing of personally-identifiable student data is unlawful under this chapter.

8 (i) When a device is permanently returned by a student, the educational institution or
9 third party who provided it shall, without otherwise accessing the data on the device, fully erase
10 all the data stored on the device and return the device to its default factory settings.

11 **16-107-3. Use of data on take-home technology.**

12 (a) Where an educational institution or third party provides a student with a technological
13 device pursuant to a take-home technology program, no school employee or third party may
14 access such a device or the data thereupon, either remotely or in person, except in accordance
15 with the provisions of this chapter.

16 (b) No school employee or third party may access any data input into, stored upon, or
17 sent or received by a student's device, including its browser, keystroke or location history, unless:

18 (1) A school employee or third party has been authorized to access specific data by a
19 student and their parent or legal guardian pursuant to a valid opt-in agreement, and access is
20 limited to that purpose;

21 (2) A school employee has reasonable suspicion that the student has violated or is
22 violating a school policy and that data on the device contains evidence of the suspected violation,
23 subject to the following limitations:

24 (i) Prior to searching a student's device based on reasonable suspicion, the school
25 employee shall document the reasonable suspicion and notify the student's parent or legal
26 guardian of the suspected violation and what data will be accessed in searching for evidence of
27 the violation;

28 (ii) Searches of a student's device based upon a reasonable suspicion of a school policy
29 violation shall be strictly limited to finding evidence of the suspected policy violation; and

30 (iii) Where a student is suspected of illegal conduct, no search may occur unless a judicial
31 warrant has been secured, even if the student is also suspected of a related or unrelated violation
32 of school policy;

33 (3) A school employee or law enforcement official reasonably suspects the student has
34 engaged or is engaging in illegal conduct, reasonably suspects data on the device contains

1 evidence of the suspected illegal conduct, and has secured a judicial warrant for a search of the
2 device;

3 (4) Doing so is necessary to update or upgrade the device's software and access is limited
4 to that purpose; or

5 (5) Doing so is necessary in response to an imminent threat to life or safety and access is
6 limited to that purpose.

7 **16-107-4. Follow up required after accessing a service.**

8 (a) Within seventy-two (72) hours of accessing a device's location tracking technology in
9 response to an imminent threat to life or safety, the school employee or law enforcement official
10 who accessed the device shall provide the student whose device was accessed, their parent or
11 legal guardian and the educational institution a written explanation of the precise threat that
12 prompted the access and what data and features were accessed.

13 (b) No school employee or third party may use a device's location tracking technology to
14 track a device's real-time or historical location, unless:

15 (1) Such use is ordered pursuant to a judicial warrant;

16 (2) The student to whom the device was provided, or their parent or legal guardian, has
17 notified a school employee or law enforcement official in writing that the device is missing or
18 stolen; or

19 (3) Doing so is necessary in response to an imminent threat to life or safety and access is
20 limited to that purpose.

21 (c) No personally-identifiable student data obtained or received from a device by a school
22 employee or authorized third party may be sold, shared, or otherwise transferred to another third
23 party, except pursuant to a valid opt-in agreement or other express authorization from a student
24 and their parent or legal guardian.

25 **16-107-5. Remote access prohibited.**

26 (a) No educational institution or third party shall activate or access any audio or video
27 receiving, transmitting, or recording functions on a student's device, unless:

28 (1) A student initiates a video chat or audio chat for educational purposes and access is
29 limited to that purpose;

30 (2) The activation and/or access is ordered pursuant to a judicial warrant; and

31 (3) Doing so is necessary in response to an imminent threat to life or safety and access is
32 limited to that purpose:

33 (b) Within seventy-two (72) hours of accessing a device's audio or video receiving,
34 transmitting, or recording functions in response to an imminent threat to life or safety, the school

1 employee or law enforcement official who accessed the device shall provide the student whose
2 device was accessed, their parent or legal guardian and the educational institution a written
3 explanation of the precise threat that prompted the access and what data and features were
4 accessed.

5 (c) This section shall not apply to video chats, audio chats or file transfers initiated by a
6 student for educational purposes and with the consent of a parent or guardian.

7 **16-107-6. Reasonable suspicion required for searches.**

8 (a) No educational institution shall search the contents of a device absent reasonable
9 suspicion that a student has engaged in misconduct.

10 (b) Educational institutions shall, as soon as practicable, but no later than forty-eight (48)
11 hours after a search has taken place, notify a student's parent or legal guardian in writing that a
12 search was conducted, and the reasons for the search.

13 (c) This shall not include instances when the student's parent or legal guardian consents
14 to a search.

15 **16-107-7. Parental disabling of Internet filtering software.**

16 Every educational institution issuing a device shall establish a procedure for parents
17 and/or legal guardians to request that a blocked website be unblocked in a timely manner, and in
18 no case shall the time to unblock a website be longer than two (2) business days.

19 **16-107-8. Location tracking of devices prohibited.**

20 No educational institution shall engage in location tracking of a device without the
21 written consent of a child's parent or legal guardian, unless the device has been reported stolen
22 and a police report has been filed with the local police department.

23 **16-107-9. Training.**

24 Notwithstanding any other provisions of this chapter, no school employee may supervise,
25 direct, or participate in a take-home technology program or access any device or data thereupon
26 until they have received adequate training to ensure understanding in compliance with the
27 provisions of this chapter.

28 **16-107-10. Penalties.**

29 In any civil action alleging a violation of this chapter, the court may:

30 (1) Award to a prevailing applicant or student declaratory relief, damages, and reasonable
31 attorneys' fees and costs; and

32 (2) Award injunctive relief against any school or agent of any educational institution that
33 or who commits or proposes to commit a violation of this chapter.

1 SECTION 2. This act shall take effect upon passage.

=====
LC001954
=====

EXPLANATION
BY THE LEGISLATIVE COUNCIL
OF

A N A C T

RELATING TO EDUCATION -- PROTECTING STUDENT PRIVACY ON SCHOOL-
OWNED TECHNOLOGY

1 This act would establish certain student privacy rights in regard to take-home technology
2 devices from school. The act would limit the ability of school officials to monitor and search a
3 student's take-home technology device and would establish the process and criteria which school
4 officials must follow to access a student's take-home technology device.

5 This act would take effect upon passage.

=====
LC001954
=====