

2020 -- H 7509

=====
LC004141
=====

STATE OF RHODE ISLAND

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2020

—————
A N A C T

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

Introduced By: Representatives Speakman, Ajello, Donovan, Kislak, and Ruggiero

Date Introduced: February 07, 2020

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 110

4 STUDENT PRIVACY IN TAKE-HOME TECHNOLOGY PROGRAMS

5 **16-110-1. Definitions.**

6 For the purposes of this chapter:

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

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

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,
2 including 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 or activate any visual or aural
4 recording or monitoring devices.

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

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

9 **16-110-2. Optional participation in take-home technology programs.**

10 (a) No educational institution shall compel, coerce, or require a student to participate in a
11 take-home technology program in the absence of a signed opt-in agreement.

12 (b) A valid opt-in agreement shall identify, with specificity:

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

14 (2) The name of the school employee(s) or third party to whom the authority to access the
15 device is being granted;

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

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

20 (c) No device or other educational benefit may be withheld from, or punitive measure
21 taken against, a student or their parent or legal guardian based in whole or in part upon a student's
22 refusal to open, close, or maintain an e-mail or other electronic communications or social media
23 account with a specific service provider.

24 (d) Where a take-home technology program is offered at an educational institution, the
25 program shall comply with chapter 104 of this title.

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

29 **16-110-3. Use of data on take-home technology.**

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

34 (b) No school employee or third party may access any data input into, stored upon, or

1 sent or received by a student's device, including its browser, keystroke or location history, unless:

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

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

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

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

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

17 (3) A school employee or law enforcement official reasonably suspects the student has
18 engaged or is engaging in illegal conduct, reasonably suspects data on the device contains
19 evidence of the suspected illegal conduct, and has secured a judicial warrant for a search of the
20 device;

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

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

25 **16-110-4. Follow up required after accessing a service.**

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

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

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

34 (2) The student to whom the device was provided, or their parent or legal guardian, has

1 notified a school employee or law enforcement official in writing that the device is missing or
2 stolen; or

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

5 **16-110-5. Remote access prohibited.**

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

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

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

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

13 (b) Within seventy-two (72) hours of accessing a device's audio or video receiving,
14 transmitting, or recording functions in response to an imminent threat to life or safety, the school
15 employee or law enforcement official who accessed the device shall provide the student whose
16 device was accessed, their parent or legal guardian and the educational institution a written
17 explanation of the precise threat that prompted the access and what data and features were
18 accessed.

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

21 **16-110-6. Reasonable suspicion required for searches.**

22 (a) No educational institution shall otherwise engage in remote access to search the
23 contents of a device absent reasonable suspicion that a student has engaged in misconduct.

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

27 (c) This shall not include instances when the student's parent or legal guardian consents
28 to a search after being provided a specific reason for the request.

29 **16-110-7. Parental disabling of Internet filtering software.**

30 Every educational institution issuing a device shall allow parents and/or legal guardians
31 to request that a blocked website be unblocked in a timely manner in accordance with any
32 established procedures pursuant to chapter 21.6 of this title.

33 **16-110-8. Location tracking of devices prohibited.**

34 No educational institution shall engage in location tracking of a device without the

1 written consent of a child's parent or legal guardian, unless the device has been reported stolen
2 and a police report has been filed with the local police department, a student has failed to return
3 the device to the institution in a timely manner, or doing so is necessary in response to an
4 imminent threat to life or safety.

5 **16-110-9, Penalties.**

6 (a) In any civil action alleging a violation of this chapter, the court may:

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

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

11 (b) The rights provided a parent or legal guardian under this chapter shall accrue to any
12 student who is eighteen (18) years of age or older.

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

=====
LC004141
=====

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 provide that no educational institution shall compel students to participate
2 in a take-home technology program (e.g., computers). This act would also provide student
3 privacy rights in the digital information contained on the computer. Access to the students'
4 information on the computer by school officials, law enforcement and third parties is limited to
5 specified circumstances.

6 This act would take effect upon passage.

=====
LC004141
=====