

HOUSE No. 3605

The Commonwealth of Massachusetts

PRESENTED BY:

Carolyn C. Dykema

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act protecting student privacy.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
<i>Carolyn C. Dykema</i>	<i>8th Middlesex</i>	<i>1/23/2015</i>
<i>Donald H. Wong</i>	<i>9th Essex</i>	<i>8/2/2019</i>

HOUSE No. 3605

By Ms. Dykema of Holliston, a petition (subject to Joint Rule 12) of Carolyn C. Dykema and Donald H. Wong relative to student privacy. Education.

The Commonwealth of Massachusetts

**In the One Hundred and Eighty-Ninth General Court
(2015-2016)**

An Act protecting student privacy.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

1 SECTION 1. The General Laws are hereby amended by inserting after section 94 of
2 chapter 71 the following section:-

3 Section 95.

4 (a) For the purposes of this section, the following words shall have the following
5 meanings:--

6 “Personally identifiable student data”, one or more of the following:

7 (1) A student’s name;

8 (2) The name of a student’s parent, legal guardian, or other family member;

9 (3) The address of a student or student’s parent, legal guardian, or other family member;

10 (4) Indirect identifiers, including a student’s date of birth, place of birth, social security
11 number, telephone number, credit card account number, insurance account number, financial
12 services account number, email address, social media address, and other electronic address; or

13 (5) Any other information that, alone or in combination, is linked or linkable to a specific
14 student that would allow a third party to identify the student with reasonable certainty.

15 “Personal device”, a technological device owned, leased, or lawfully possessed by a
16 student that was not provided to the student by the school or school district.

17 “Technological device”, any computer, cellular phone, smartphone, digital camera, video
18 camera, audio recording device, or other electronic device that can be used for creating, storing,
19 or transmitting information in the form of electronic data.

20 “Third party”, any person or entity other than a school employee, student, or parent or
21 legal guardian of a student.

22 (b) Educational institutions shall have the discretion to limit or prohibit the possession or
23 use of certain personal devices by students on school property. A violation of such a limitation
24 or prohibition shall not be the sole basis for a reasonable suspicion to access the device.

25 (c) No school employee or third party shall access any data or other content input into or
26 stored upon a personal device of a student, notwithstanding any violation of school code of
27 conduct provisions regarding possession or use of such device, unless:

28 (1) A school employee has a reasonable suspicion that a student has violated or is
29 violating a separate provision of the code of conduct and that the device contains evidence
30 thereof, subject to the following limitations:

31 (i) Searches of shall be conducted only of personal devices located on school
32 property.

33 (ii) Prior to searching a student's personal device based on reasonable suspicion, the
34 school employee shall document such reasonable suspicion and notify the student and the
35 student's parent or legal guardian of the suspected violation and the type of data sought to be
36 accessed in searching for evidence of the violation.

37 (iii) Searches of a student's personal device based on reasonable suspicion shall be
38 strictly limited to locating evidence of the particular suspected policy violation.

39 (iv) Where a student is suspected of conduct which is a criminal offense under the
40 general laws, no search shall be undertaken without the authorization of a valid judicial warrant
41 secured in accordance with subsection (c)(2), notwithstanding any suspected violation of the
42 school code of conduct.

43 (2) Authorized by a valid warrant for the search of the device issued pursuant to the
44 requirements of sections 2 through 3A of chapter 276; or

45 (3) Accessing a student's personal device is necessary in response to an imminent threat
46 to life or safety. Within 72 hours of accessing a personal device in response to an imminent
47 threat to life or safety, the school employee or law enforcement official who accessed the device
48 shall provide the student whose device was accessed, the student's parent or legal guardian, and
49 the educational institution a written description of the particular threat and the data accessed.

50 (d) Evidence or information obtained or collected in violation of this section shall not be
51 admissible as evidence in any civil or criminal trial or legal proceeding, disciplinary action, or
52 administrative hearing.