

HOUSE No. 440

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 to protect student privacy.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
<i>Carolyn C. Dykema</i>	<i>8th Middlesex</i>
<i>James B. Eldridge</i>	<i>Middlesex and Worcester</i>
<i>Michael O. Moore</i>	<i>Second Worcester</i>
<i>Tommy Vitolo</i>	<i>15th Norfolk</i>
<i>Marjorie C. Decker</i>	<i>25th Middlesex</i>
<i>Rebecca L. Rausch</i>	<i>Norfolk, Bristol and Middlesex</i>
<i>Mindy Domb</i>	<i>3rd Hampshire</i>
<i>Denise Provost</i>	<i>27th Middlesex</i>
<i>David Allen Robertson</i>	<i>19th Middlesex</i>
<i>Sean Garballey</i>	<i>23rd Middlesex</i>
<i>David M. Rogers</i>	<i>24th Middlesex</i>
<i>Paul Brodeur</i>	<i>32nd Middlesex</i>

HOUSE No. 440

By Ms. Dykema of Holliston, a petition (accompanied by bill, House, No. 440) of Carolyn C. Dykema and others for legislation to prohibit school administrators and other employees from searching the personal mobile devices of students without reasonable cause. Education.

The Commonwealth of Massachusetts

**In the One Hundred and Ninety-First General Court
(2019-2020)**

An Act to protect 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. Chapter 71 of the General Laws, as appearing in the 2016 Official Edition,
2 is hereby amended by adding the following section:-

3 Section 98.

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

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

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

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

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

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

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

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

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

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

29 (iv) Where a student is suspected of conduct which is a criminal offense under the
30 general laws, no search shall be undertaken without the authorization of a valid judicial warrant

31 secured in accordance with subsection (c)(2), notwithstanding any suspected violation of the
32 school code of conduct.

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

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

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