

HOUSE No. 588

The Commonwealth of Massachusetts

PRESENTED BY:

Aaron Vega, (BY REQUEST)

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 requiring privacy protections and supporting safer technology in schools.

PETITION OF:

NAME:

DISTRICT/ADDRESS:

Kristin Beatty

HOUSE No. 588

By Mr. Vega of Holyoke (by request), a petition (accompanied by bill, House, No. 588) of Kristin Beatty relative to requiring privacy protections and supporting safer technology in schools. Education.

The Commonwealth of Massachusetts

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

An Act requiring privacy protections and supporting safer technology in schools.

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 is hereby amended by striking the
2 language of Section 93 and inserting thereof the following:-

3 SECTION 93. TECHNOLOGY PRIVACY AND SAFETY MEASURES FOR
4 EDUCATION

5 (a) As used in this section, the following words shall have the following meanings:

6 “Confidential data” is data collected on students or staff and which includes:

7 (1) standard identifying information:

8 i. names of staff and students

9 ii. dates of birth

10 iii. addresses

- 11 iv. grades
- 12 v. medical information
- 13 vi. exam results
- 14 vii. staff development reviews
- 15 viii. assessments
- 16 ix. other personal identifying information

17 (2) identifying data such as location-tracking, photographs, and biometric data, which
18 includes unique biological identifiers such as voice audio or fingerprints

19 (3) personal writings or other personal work such as art

20 (4) political views

21 (5) socioeconomic data

22 (6) disciplinary data

23 (7) similar data or information on other individuals that are not students or staff, but may
24 be referenced in or extracted from student and staff data.

25 (8) observed and inferred data from the data provided

26 “Granular opt-out processes for different uses of data” is providing separate options to
27 refuse different types of data sharing. Considerations include but are not limited to placement in
28 a yearbook or directory, using cloud services, or using school-issued devices or personal devices.

29 “Opt-out alternatives for technology” is an opt-out of using technology with a
30 comparable or alternative non-technological assignment.

31 “Students and staff” includes all students in pre-K through 12th grade, including students
32 in home schooling, as well as preK through 12th grade staff and teachers, including tutors and
33 extra-curricular leaders. Tutors or other arranged staff, including legal guardians or volunteers,
34 that provide extra-curricular activities or other educational learning, are also included.

35 “School vendors and schools” includes schools and vendors for schools serving PreK-12
36 students and staff, including home school vendors, legal guardians, volunteers, or tutors
37 providing educational services and extra-curricular activities.

38 (b) No contract shall breach this section for the protection of students and staff.

39 Use of confidential data from students and staff for marketing, political identification,
40 and abuse or other mistreatment shall be unlawful outside of reasonable public records used for
41 political identification.

42 Storage of confidential data from students and staff shall be unlawful outside of needs
43 specific to educational, legal, and government purposes; reasonable knowledge acquired based
44 on personal relationships; and, when not extraneous to the product sold, business needs.

45 Collecting and storing student biometric data shall be unlawful; provided, however, that
46 temporary collection of a student photo for ID or printing in a yearbook shall be allowed, and
47 students may opt-in to take and keep personal photographs, video, and audio recordings, or opt in
48 for public photographs and video recordings. The same parameters as for students shall apply for
49 staff biometric data, provided, however, that exemptions may exist only as stipulated under state

50 law for the Department of Criminal Justice to collect biometric data from staff, including
51 volunteers, for criminal background checks.

52 Except as necessary for defined and reasonable bureaucratic, legal, health, safety or
53 educational functions of a school and values of a democratic state, the gathering, sharing, or
54 storing of confidential data on school students and staff in the Commonwealth shall be unlawful,
55 and data must be kept anonymous when personal identifying information is not relevant or
56 necessary to the data collection. Data collection limits shall not impair schools from retaining
57 data necessary to function as a school or comply with legal, employment, and safety needs.
58 School vendors and schools shall collect only as much information as needed to do a particular
59 assigned task, take steps to avoid placing confidential data at risk, and, when the information is
60 no longer required, insure data is shredded or otherwise securely erased within a reasonable time
61 frame. School vendors may not claim ignorance, but shall be responsible for protecting school
62 and staff privacy as well as safety.

63 Neither shall a school nor a district require teachers or students to enroll in digital
64 systems that transfer their intellectual property rights to a private corporation, nor shall a district
65 or school sell or license a teacher's or student's personal information to any third party for any
66 reason or make it available for marketing or commercial purposes.

67 The district shall provide annual training to all staff on the protection of teacher and
68 student data, federal and state privacy laws, best practices for protection of education-related
69 data, and best practices for addressing technological health and safety concerns.

70 It shall be unlawful to mandate the posting of primary and secondary student work online
71 or in public spaces as a condition of mandatory course work. It shall be unlawful as a condition

72 of employment to mandate the posting of school staff confidential data or intellectual property
73 online or in public spaces, excepting staff names and, when appropriate, credentials, contact
74 information, and relevant research, interests, or studies. Posting student images or work online or
75 in public spaces shall be lawful only with the directly specified consent of the student and
76 relevant legal guardian. Requests for permission to post student work or images must be related
77 to a specific request and for specific platforms, to avoid blanket permission statements for all
78 platforms and all types of materials.

79 Schools shall act responsibly to protect student and staff privacy, health and safety, and
80 shall respect the wishes of legal guardians to limit preK-12 student technological use,
81 particularly in regard to privacy, safety, or health. Considerations to protect student and staff
82 privacy, safety, and health include but are not limited to the following:

- 83 1. Hardwiring internet connections and technological equipment rather than using
84 wireless; and
- 85 2. Limiting use of technology within the school to small prescribed and well-
86 monitored settings to restrict misuse and enable greater quality control of equipment; and
- 87 3. Isolating confidential data and equipment from less secure systems and the
88 Internet; and
- 89 4. Avoiding or appropriately segregating and labeling technologies in student and
90 staff areas which have the ability to record audio, images, or other confidential data; and
- 91 5. Decommissioning devices and equipment which pose risks; and
- 92 6. Installing software and equipment with credible privacy protections; and

- 93 7. Establishing granular opt-out processes for different uses of data; and
- 94 8. Providing student opt-out alternatives for technology; and
- 95 9. Avoiding technological storage of confidential data; and
- 96 10. Limiting reliance on and excessive use of technology; and
- 97 11. Storing research data anonymously or rejecting research studies which pose
98 confidentiality risks; and
- 99 12. Following traditional practices of requiring warrants or informed legal guardian
100 consent for release of confidential data.

101 SECTION 2. Section 1I of chapter 69 of the General Laws, as appearing in Title XII of
102 Part I the 2017 Official Edition, is hereby amended by striking out paragraph five and inserting
103 in place thereof the following paragraph:-

104 The commissioner is authorized and directed to gather only the necessary information,
105 including the information specified herein and such other information as the board shall require,
106 for the purposes of evaluating individual public schools, school districts, and the efficacy and
107 equity of state and federal mandated programs. The commissioner is instructed to emphasize
108 evaluation measures that protect student and staff privacy and safety, and limit other bureaucratic
109 requests. All information filed pursuant to this section shall be filed in the manner and form
110 prescribed by the department that best protects the privacy of students and staff while insuring
111 that data collection is minimized and storage facilities & procedures secure.

112 SECTION 3. Section 1I of chapter 69 of the General Laws, as appearing in Title XII of
113 Part I the 2017 Official Edition, is hereby amended by inserting after the fifth paragraph the
114 following paragraphs:-

115 The commissioner is to comply with all state and federal laws to protect student and staff
116 privacy in establishing such a system, and shall as a matter of policy avoid placing sensitive
117 documents online and avoid collecting nonessential data. The commissioner shall not collect
118 biometric data as a function of school assessment or education, nor shall the commissioner
119 collect or access biometric data from students or staff for any other purpose; provided, however,
120 that collection of biometric data by the Department of Criminal Justice may be required under
121 state law for criminal background checks of school and district staff, including volunteers. The
122 commissioner shall periodically review and destroy outdated and irrelevant documents contained
123 in the temporary record.

124 The commissioner shall provide annual training to relevant personnel on the protection of
125 teacher and student data, federal and state privacy laws, and best practices for protection of
126 education-related data, and shall provide for informational and training materials on the subject
127 to be available for use by Commonwealth schools. Such training and informational materials
128 shall not serve to favor a particular vendor or business, and any promotion of an investment or
129 business tied to the persons with the Board of Education or to the governor or secretary of state
130 shall be accompanied by a disclaimer noting the connection.

131 SECTION 5. Section 1I of chapter 69 of the General Laws, as appearing in Title XII of
132 Part I the 2017 Official Edition, is hereby amended by striking out paragraph seven and inserting
133 in place thereof the following paragraph:-

134 Each school district shall maintain individual records on every student and employee.
135 Each student record shall contain a unique and confidential identification number, basic
136 demographic information, program, and course information. School districts, charter schools, the
137 board, and the Department of Elementary and Secondary Education shall limit collection and
138 storage of data to that clearly necessary to allow for student transcripts, evaluations of schools,
139 and improvement of education, and shall avoid collection of personal and behavioral student data
140 other than that required for transcripts. The department shall also discourage collection of
141 personal and behavioral data on staff by school districts or charter schools, except as part of
142 reasonable evaluations as approved by a school, district, or the department. The board and
143 Department of Elementary and Secondary Education shall have as a goal the avoidance of
144 collecting extraneous or personal data on students and staff that can be mined for observed and
145 inferred data, and note that extraneous data is that which is not necessary to accomplish its
146 educational function. With this goal of privacy protection in mind, the board and Department of
147 Elementary and Secondary Education shall seek performance measures and procedures that
148 respect privacy and defer, when appropriate, data collection besides rejecting vulnerable storage
149 facilities.