HOUSE DOCKET, NO. 1003 FILED ON: 1/15/2019

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:	DATE ADDED:
Kristin Beatty		*1/15/2019*

HOUSE DOCKET, NO. 1003 FILED ON: 1/15/2019

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:

SECTION 1. Chapter 71 of the General Laws is hereby amended by striking the language of Section 93 and inserting thereof the following:-

SECTION 93. TECHNOLOGY PRIVACY AND SAFETY MEASURES FOR EDUCATION

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

"Confidential data" is data collected on students or staff and which includes:

(1) standard identifying information:

i. names of staff and students

ii. dates of birth

iii. addresses

iv. grades

v. medical information

vi. exam results

vii. staff development reviews

viii. assessments

ix. other personal identifying information

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

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

(4) political views

(5) socioeconomic data

(6) disciplinary data

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

(8) observed and inferred data from the data provided

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Hardwiring internet connections and technological equipment rather than using wireless; and

2. Limiting use of technology within the school to small prescribed and well-monitored settings to restrict misuse and enable greater quality control of equipment; and

3. Isolating confidential data and equipment from less secure systems and the Internet; and

4. Avoiding or appropriately segregating and labeling technologies in student and staff areas which have the ability to record audio, images, or other confidential data; and

5. Decommissioning devices and equipment which pose risks; and

6. Installing software and equipment with credible privacy protections; and

7. Establishing granular opt-out processes for different uses of data; and

8. Providing student opt-out alternatives for technology; and

9. Avoiding technological storage of confidential data; and

10. Limiting reliance on and excessive use of technology; and

11. Storing research data anonymously or rejecting research studies which pose confidentiality risks; and

12. Following traditional practices of requiring warrants or informed legal guardian consent for release of confidential data.

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

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

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

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

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

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

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