

**SENATE . . . . . No.**

---

**The Commonwealth of Massachusetts**

\_\_\_\_\_

PRESENTED BY:

***Barry R. Finegold***

\_\_\_\_\_

*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 establishing privacy standards for student and educator data.

\_\_\_\_\_

PETITION OF:

NAME:

*Barry R. Finegold*

DISTRICT/ADDRESS:

*Second Essex and Middlesex*

SENATE . . . . . No.

[Pin Slip]

[SIMILAR MATTER FILED IN PREVIOUS SESSION  
SEE SENATE, NO. 280 OF 2023-2024.]

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Fourth General Court  
(2025-2026)

An Act establishing privacy standards for student and educator data.

*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 inserting after  
2 section 34H the following 4 sections:-

3 Section 34I. As used in sections 34I through 34L, inclusive, the following words shall,  
4 unless the context clearly requires otherwise, have the following meanings:

5 “Aggregated data”, data collected and reported at the group, cohort, school, school  
6 district, region or state level that is aggregated using protocols that are both intended and  
7 reasonably likely to preserve the anonymity of each individual.

8 “Board”, the board of elementary and secondary education.

9 “Commissioner”, the commissioner of the department of elementary and secondary  
10 education.

11 "Covered information", information, data or records, inclusive of student records as  
12 defined in the board's regulations, that, alone or in combination, can be used to identify a  
13 specific student, teacher, principal, administrator or student's family member and that is: (i)  
14 created by or provided to an operator by a student, or the student's parent or legal guardian, in the  
15 course of the student's, parent's or legal guardian's use of the operator's site, service or  
16 application for K-12 school purposes; (ii) created by or provided to an operator by an employee  
17 or agent of a school district or K-12 school for K-12 school purposes; (iii) gathered by an  
18 operator through the operation of its site, service or application for K-12 school purposes and  
19 personally identifies a student; or (iv) gathered by an operator through the operation of its site,  
20 service or application in connection with performance evaluations conducted pursuant to section  
21 38 and that personally identifies a teacher, principal or administrator.

22 For a student, covered information includes, but is not limited to, information in the  
23 student's educational record or electronic mail, including student-generated work; first and last  
24 name; home address and geolocation information; telephone number; electronic mail address or  
25 other information that allows physical or online contact; discipline records; test results, grades  
26 and student evaluations; special education data; juvenile dependency records; criminal records;  
27 medical records and health records; social security number; student identifiers; biometric  
28 information; socioeconomic information; food purchases; political and religious affiliations; text  
29 messages; student identifiers; search activity and online behavior or usage of applications when  
30 linked or linkable to a student; photographs; voice recordings; and persistent unique identifiers.

31 "De-identified data", records and information from which all personally identifiable  
32 information has been removed or obscured such that the remaining information does not

33 reasonably identify a specific individual including, but not limited to, any information that alone  
34 or in combination is linkable to a specific individual.

35 “Department”, the department of elementary and secondary education.

36 “Destroy”, action taken in the normal course of business that is intended, and would be  
37 believed by a reasonable person in the context of the information’s medium, to make such  
38 information permanently irretrievable.

39 “District” or “school district”, the school department of a city or town, regional school  
40 district, vocational or agricultural school, independent vocational school or charter school.

41 “Educational entity”, a state educational agency, school district, K-12 school or  
42 subdivision thereof, education collaborative as defined in section 4E of chapter 40, approved  
43 public or private day or residential school providing special education services to publicly  
44 funded eligible students pursuant to chapter 71B or institutional K-12 school program overseen  
45 by a state agency including the department of youth services, the department of mental health or  
46 the department of public health as well as employees acting under the authority or on behalf of  
47 an educational entity.

48 “K-12 school”, a school that offers any of grades kindergarten to 12 and that is operated  
49 by a school district; provided, however, that a K-12 school shall include any preschool or  
50 prekindergarten program or course of instruction provided by a school district.

51 “K-12 school purposes”, uses that are directed by or that customarily take place at the  
52 direction of a school district, K-12 school or teacher or that aid in the administration of school  
53 activities including, but not limited to, instruction in the classroom or at home, administrative

54 activities and collaboration between students, school personnel or parents, or that are otherwise  
55 for the use and benefit of the K-12 school; provided, however, that K-12 school purposes shall  
56 include comparable purposes in the administration of any preschool or prekindergarten program  
57 or course of instruction provided by a school district.

58 “Operator”, a person or entity operating in accordance with an agreement with an  
59 educational entity to provide an internet website, online service, online application or mobile  
60 application for K-12 school purposes or at the direction of an educational entity or an employee  
61 of an educational entity; provided, however, that this definition shall not apply to the department,  
62 school district, K-12 school or other educational entity.

63 “Persistent unique identifier”, an identifier that can be used to recognize a consumer, a  
64 family or a device that is linked to a consumer or family over time and across different services,  
65 including, but not limited to: (i) a device identifier; (ii) an Internet Protocol address; (iii) cookies,  
66 beacons, pixel tags, mobile ad identifiers or similar technology; (iv) customer number, unique  
67 pseudonym or user alias; or (v) telephone number or other forms of persistent or probabilistic  
68 identifiers that can be used to identify a particular consumer or device; provided, however, that  
69 for the purposes of this definition “family” shall mean a custodial parent or guardian and any  
70 minor children over which the parent or guardian has custody.

71 “Targeted advertising”, presenting or serving advertisements to a student where the  
72 substance, time or manner of the advertisement is determined based in whole or in part on  
73 information obtained or inferred over time from that student's online behavior, usage of  
74 applications or covered information. It does not include advertising to a student at an online  
75 location based upon that student's current visit to that location or in response to that student’s

76 request for information or feedback without the retention of that student's online activities or  
77 requests over time for the purpose of targeting subsequent advertisements.

78 Section 34J. (a) An operator shall not, with respect to its site, service or application:

79 (i) engage in targeted advertising on the operator's site, service or application, or targeted  
80 advertising on any other site, service or application if the targeting of the advertising is based on  
81 any information, including covered information or persistent unique identifiers, that the operator  
82 has acquired because of the use of that operator's site, service or application for K-12 school  
83 purposes;

84 (ii) use covered information, including persistent unique identifiers, created or gathered  
85 by the operator's site, service or application, to amass a profile about a student or a teacher,  
86 principal or administrator except in furtherance of K-12 school purposes;

87 (iii) sell or rent a student's information, including covered information; provided,  
88 however, that this clause shall not apply to the purchase, merger or other type of acquisition of  
89 an operator by another entity if the operator or successor entity complies with sections 34I  
90 through 34L, inclusive, or to national assessment providers if the national assessment provider  
91 secures the express written consent of the parent or student, if such student is not less than 18  
92 years old, given in response to clear and conspicuous notice solely to provide access to  
93 employment, educational scholarships or financial aid or postsecondary educational  
94 opportunities; or

95 (iv) disclose covered information; provided, however, that an operator may disclose  
96 covered information of a student so long as clauses (i) through (iii), inclusive, of this subsection  
97 are not violated, under the following circumstances:

98 (A) if provisions of federal or state law require the operator to disclose the information  
99 and the operator complies with the requirements of federal and state law in protecting and  
100 disclosing that information;

101 (B) for research purposes with the approval of the relevant educational entity and in  
102 compliance with and subject to the restrictions of state and federal law; provided, however, that  
103 the information shall be de-identified prior to being disclosed and that the operator shall share  
104 research results with the educational entity in advance of any public dissemination; or

105 (C) to an educational entity, including a K-12 school and school district, for K-12 school  
106 purposes, as permitted by state or federal law.

107 (b) An operator shall:

108 (i) implement and maintain reasonable security procedures and practices appropriate to  
109 the nature of the covered information designed to protect that covered information from  
110 unauthorized access, destruction, use, modification or disclosure and in compliance with  
111 regulations promulgated by the board pursuant to section 34L; and

112 (ii) immediately return or destroy covered information if requested by the educational  
113 entity or when covered information is no longer required for K-12 school purposes or other  
114 lawful purposes, such as complying with a judicial order or law enforcement request.

115 (c) Subject to the provisions of this section, an operator may use de-identified data to  
116 maintain, develop, support, improve or diagnose the operator's site, service or application.

117 Subject to the provisions of this section, an operator may use aggregated or de-identified student  
118 information to demonstrate the effectiveness of the operator's products or services, including

119 marketing or within the operator’s site, service or application or other sites, services or  
120 applications owned by the operator to improve educational purposes.

121 (d) Nothing in this section shall be construed to: (i) limit the authority of a law  
122 enforcement agency to obtain any content or information from an operator as authorized by law  
123 or pursuant to an order of a court of competent jurisdiction; (ii) limit the ability of an operator to  
124 use student data, including covered information, for adaptive learning or customized student  
125 learning purposes; (iii) apply to general audience Internet websites, general audience online  
126 services, general audience online applications or general audience mobile applications, even if  
127 login credentials created for an operator’s site, service or application may be used to access those  
128 general audience sites, services or applications; (iv) limit service providers from providing  
129 Internet connectivity to schools or students and their families; (v) prohibit an operator of an  
130 Internet website, online service, online application or mobile application from marketing  
131 educational products directly to parents if the marketing did not result from the use of covered  
132 information obtained by the operator through the provision of services covered under this  
133 section; (vi) impose a duty upon a provider of an electronic store, gateway, marketplace or other  
134 means of purchasing or downloading software or applications to review or enforce compliance  
135 with this section on those applications or software; or (vii) prohibit students from downloading,  
136 exporting, transferring, saving or maintaining their own data or documents.

137 (e) An aggrieved student or educational entity may institute a civil action against an  
138 operator for damages or to restrain a violation of this section and may recover: (i) not more than  
139 \$10,000 for each disclosure that violates this section; (ii) not more than \$10,000 for each adverse  
140 action that violates this section, or actual damages, whichever amount is higher; (iii) punitive



141 damages if a court determines that a violation was willful; and (iv) reasonable attorneys' fees and  
142 other litigation costs reasonably incurred.

143 (f) The commissioner may bar an operator that improperly discloses covered information  
144 from receiving access to student or educator evaluation records of any educational entity in the  
145 commonwealth for a period of not less than 5 years.

146 Section 34K. (a) Any contract or agreement that is entered between an educational entity  
147 and an operator, as defined in section 34I, pursuant to which the operator sells, leases, provides,  
148 operates or maintains a service that grants access to covered information or creates any covered  
149 information, including, but not limited to any cloud-based services for the digital storage,  
150 management and retrieval of pupil records or any digital software that authorizes an operator to  
151 access and acquire student records, shall contain:

152 (i) a description of the covered information collected, stored and managed and a  
153 statement that covered information and student records continue to be the property and under the  
154 control of the educational entity;

155 (ii) a prohibition against the operator using covered information for commercial or  
156 advertising purposes or for any purpose other than K-12 school purposes;

157 (iii) a description of the procedures by which a parent, legal guardian or eligible student  
158 may review the student's records and work with the educational entity to correct erroneous  
159 information, in accordance with state and federal law;

160 (iv) a requirement that only persons, whether they are employees of the operator or other  
161 persons, such as employees of subcontractors, with a legitimate need to access covered

162 information to support professional roles consistent with the terms of the contract or agreement  
163 and federal and state law shall have access to it, with either the identification of said persons or  
164 an agreement to identify said persons upon request;

165 (v) a description of the reasonable administrative, technical and physical safeguards,  
166 including with respect to encryption technology to protect covered information while in motion  
167 or in the operator's custody, that the operator will employ to protect the security, confidentiality  
168 and integrity of covered information in its custody; provided, however, that compliance with this  
169 requirement shall not, in itself, absolve the operator of liability in the event of an unauthorized  
170 disclosure of covered information;

171 (vi) a description of the procedures for notifying any and all affected parties in the event  
172 of an unauthorized disclosure of covered information or any breach of security resulting in an  
173 unauthorized release of covered information, provided that such procedures shall comply with  
174 chapter 444 of the Acts of 2018 and implementing regulations;

175 (vii) a certification that covered information shall be returned or destroyed by the  
176 operator upon completion of the terms of the contract; and

177 (viii) a description of how the educational entity and the operator will jointly ensure  
178 compliance with applicable federal and state law including, but not limited to, 20 U.S.C. section  
179 1232g, 15 U.S.C. section 6501 et. seq. and sections 34A through 34L, inclusive, of this chapter.

180 (b) Any contract that fails to comply with the requirements of this section shall be  
181 voidable and all covered information and student records in possession of an operator or any  
182 third party shall be returned to the educational entity or, if the return of such information is not  
183 technologically feasible, destroyed.

184 Section 34L. (a) The board shall promulgate regulations that establish data security and  
185 privacy responsibilities of the department and educational entities, as well as minimum required  
186 security standards for operators, including for use in department and educational entity contracts  
187 and agreements with operators and shall approve the department's data privacy and security  
188 policy and security plan for the commonwealth's data system. The regulations shall further  
189 establish a process through which the commissioner, pursuant to subsection (g) of section 34J,  
190 may bar an operator from receiving student and educator evaluation data of any educational  
191 entity in this commonwealth for a period of not less than 5 years. The regulations shall further  
192 provide that curricula in student data privacy, security and confidentiality shall be a requirement  
193 for approved educator preparation programs. In carrying out these responsibilities, the board  
194 shall consult with the executive office of technology services and security and seek the input of  
195 security and cybersecurity experts, including those from fields in addition to education that have  
196 experience with personal data protection.

197 (b) The commissioner shall appoint a chief privacy officer with experience in data  
198 privacy and security. The chief privacy officer shall oversee the development and  
199 implementation, subject to the board's approval, of a department data privacy and security policy  
200 and a detailed security plan for the commonwealth's data system in consultation with the  
201 executive office of technology services and security. The chief privacy officer shall further: (i)  
202 develop a model school district data privacy and security policy as well as a model operator  
203 contract or contracts in consultation with the executive office of technology services and  
204 security; (ii) otherwise support and supervise implementation of sections 34I through 34L,  
205 inclusive, and the regulations issued by the board pursuant to subsection (a); (iii) develop and  
206 provide a program of training, technical assistance and resource materials to K-12 schools,

207 school districts and other educational entities including through the issuance of guidance and  
208 recommendations to assist with compliance with federal and state law pertaining to personally  
209 identifiable information including, but not limited to, 20 U.S.C. 1232g, sections 34A through  
210 34L, inclusive, of this chapter, chapter 66A of the General Laws and chapter 444 of the Acts of  
211 2018; (iv) develop and oversee a program of oversight, support and accountability for the  
212 department and educational entities responsible for implementing policies pursuant to sections  
213 34I through 34L of this chapter; and (v) assist the commissioner with enforcement  
214 responsibilities regarding operators that violate any provision of sections 34I through 34K,  
215 inclusive, of this chapter.

216 (c) The department shall make publicly available a list of categories of covered  
217 information collected by the department including, but not limited to, covered information  
218 required to be collected or reported by state or federal law. The list shall contain the source of the  
219 information, the reason for the collection of the information and the use of the information  
220 collected.

221 (d) In accordance with the regulations of the board promulgated pursuant to subsection  
222 (a), each district shall develop a detailed privacy and security policy for the protection of covered  
223 information that includes security breach planning, notice and procedures; provided, however,  
224 that said policy shall include a requirement that the district report all significant data breaches of  
225 student data either by the district or an operator to the commissioner within 10 business days of  
226 the initial discovery of the significant data breach; and provided further, that a district may adopt  
227 any model policy developed by the chief privacy officer of the department and approved by the  
228 board to comply with this requirement. Each district shall designate an individual to act as a  
229 student data manager to oversee said policy.

230           (e) Each district shall make publicly available on its website a list of categories of student  
231 personally identifiable information collected at the school district, school or classroom level. The  
232 list shall contain the source of the information, the reason for collection of the information and  
233 the use of the information. Each district shall further make publicly available on its website a list  
234 of the operators with which the district has a contract or agreement that involves the creation,  
235 provision or gathering of covered information and a list of operators with which the district had a  
236 contract or agreement that involved the creation, provision or gathering of covered information  
237 in the last 10 years.

238           (f) Each district shall provide annual training regarding the confidentiality of student data  
239 to any employee with access to covered information; provided, however, that completion of said  
240 training shall be a condition of a provisional or standard educator certification as defined in  
241 section 38G.