

SENATE No. 2618

The Commonwealth of Massachusetts

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

1 by inserting at the end thereof the following section:-

2 SECTION 5. Chapter 71 of the General Laws is hereby amended by inserting after
3 section 34H the following 4 sections:-

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

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

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

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

12 "Covered information", information, data or records, inclusive of student records as
13 defined in the board’s regulations, that, alone or in combination, can be used to identify a
14 specific student, teacher, principal, administrator or student’s family member and that is: (i)
15 created by or provided to an operator by a student, or the student's parent or legal guardian, in the

16 course of the student's, parent's or legal guardian's use of the operator's site, service or
17 application for K-12 school purposes; (ii) created by or provided to an operator by an employee
18 or agent of a school district or K-12 school for K-12 school purposes; (iii) gathered by an
19 operator through the operation of its site, service or application for K-12 school purposes and
20 personally identifies a student; or (iv) gathered by an operator through the operation of its site,
21 service or application in connection with performance evaluations conducted pursuant to section
22 38 and that personally identifies a teacher, principal or administrator.

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

32 “De-identified data”, records and information from which all personally identifiable
33 information has been removed or obscured such that the remaining information does not
34 reasonably identify a specific individual including, but not limited to, any information that alone
35 or in combination is linkable to a specific individual.

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

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

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

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

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

52 “K-12 school purposes”, uses that are directed by or that customarily take place at the
53 direction of a school district, K-12 school or teacher or that aid in the administration of school
54 activities including, but not limited to, instruction in the classroom or at home, administrative
55 activities and collaboration between students, school personnel or parents, or that are otherwise
56 for the use and benefit of the K-12 school; provided, however, that K-12 school purposes shall
57 include comparable purposes in the administration of any preschool or prekindergarten program
58 or course of instruction provided by a school district.

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

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

72 “Targeted advertising”, presenting or serving advertisements to a student where the
73 substance, time or manner of the advertisement is determined based in whole or in part on
74 information obtained or inferred over time from that student's online behavior, usage of
75 applications or covered information. It does not include advertising to a student at an online
76 location based upon that student's current visit to that location or in response to that student’s
77 request for information or feedback without the retention of that student's online activities or
78 requests over time for the purpose of targeting subsequent advertisements.

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

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

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

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

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

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

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

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

108 (b) An operator shall:

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

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

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

118 Subject to the provisions of this section, an operator may use aggregated or de-identified student
119 information to demonstrate the effectiveness of the operator's products or services, including
120 marketing or within the operator's site, service or application or other sites, services or
121 applications owned by the operator to improve educational purposes.

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

138 (e) An aggrieved student or educational entity may institute a civil action against an
139 operator for damages or to restrain a violation of this section and may recover: (i) not more than
140 \$10,000 for each disclosure that violates this section; (ii) not more than \$10,000 for each adverse
141 action that violates this section, or actual damages, whichever amount is higher; (iii) punitive
142 damages if a court determines that a violation was willful; and (iv) reasonable attorneys' fees and
143 other litigation costs reasonably incurred.

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

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

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

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

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

161 (iv) a requirement that only persons, whether they are employees of the operator or other
162 persons, such as employees of subcontractors, with a legitimate need to access covered
163 information to support professional roles consistent with the terms of the contract or agreement
164 and federal and state law shall have access to it, with either the identification of said persons or
165 an agreement to identify said persons upon request;

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

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

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

178 (viii) a description of how the educational entity and the operator will jointly ensure
179 compliance with applicable federal and state law including, but not limited to, 20 U.S.C. section
180 1232g, 15 U.S.C. section 6501 et. seq. and sections 34A through 34L, inclusive, of this chapter.

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

185 Section 34L. (a) The board shall promulgate regulations that establish data security and
186 privacy responsibilities of the department and educational entities, as well as minimum required
187 security standards for operators, including for use in department and educational entity contracts

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

198 (b) The commissioner shall appoint a chief privacy officer with experience in data
199 privacy and security. The chief privacy officer shall oversee the development and
200 implementation, subject to the board's approval, of a department data privacy and security policy
201 and a detailed security plan for the commonwealth's data system in consultation with the
202 executive office of technology services and security. The chief privacy officer shall further: (i)
203 develop a model school district data privacy and security policy as well as a model operator
204 contract or contracts in consultation with the executive office of technology services and
205 security; (ii) otherwise support and supervise implementation of sections 34I through 34L,
206 inclusive, and the regulations issued by the board pursuant to subsection (a); (iii) develop and
207 provide a program of training, technical assistance and resource materials to K-12 schools,
208 school districts and other educational entities including through the issuance of guidance and
209 recommendations to assist with compliance with federal and state law pertaining to personally
210 identifiable information including, but not limited to, 20 U.S.C. 1232g, sections 34A through

211 34L, inclusive, of this chapter, chapter 66A of the General Laws and chapter 444 of the Acts of
212 2018; (iv) develop and oversee a program of oversight, support and accountability for the
213 department and educational entities responsible for implementing policies pursuant to sections
214 34I through 34L of this chapter; and (v) assist the commissioner with enforcement
215 responsibilities regarding operators that violate any provision of sections 34I through 34K,
216 inclusive, of this chapter.

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

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

231 (e) Each district shall make publicly available on its website a list of categories of student
232 personally identifiable information collected at the school district, school or classroom level. The

233 list shall contain the source of the information, the reason for collection of the information and
234 the use of the information. Each district shall further make publicly available on its website a list
235 of the operators with which the district has a contract or agreement that involves the creation,
236 provision or gathering of covered information and a list of operators with which the district had a
237 contract or agreement that involved the creation, provision or gathering of covered information
238 in the last 10 years.

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