



SPONSOR: Sen. Sokola & Rep. Jaques & Rep. Ramone
Sens. Henry, Marshall, Peterson; Reps. Briggs King,
Keeley, Lynn, Matthews, Miro, Osienki, K. Williams

DELAWARE STATE SENATE
148th GENERAL ASSEMBLY

SENATE BILL NO. 79

AN ACT TO AMEND TITLE 14 OF THE DELAWARE CODE RELATING TO EDUCATIONAL DATA
GOVERNANCE.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF DELAWARE:

1 Section 1. Amend § 4111, Title 14 of the Delaware Code by making deletions as shown by strike through
2 and insertions as shown by underline as follows:

3 § 4111. ~~Disclosure~~ Privacy, accessibility, and transparency of pupils' school-student records.

4 (a) Definitions. The following words, terms and phrases, when used in this section, shall have the meaning
5 ascribed to them except where the context clearly indicates a different meaning:

6 (1) "Aggregate student data" means data that is not personally identifiable and that is collected or
7 reported at the group, cohort, or institutional level.

8 (2) "De-identified data" means a student data set that cannot reasonably be used to identify, contact,
9 single out, or infer information about a student or device used by a student.

10 (3) "Department" means the Delaware Department of Education.

11 (4) "Education record" means an education record as defined in FERPA, the Individuals with
12 Disabilities Education Act, § 1400 of Title 20 of the United States Code and implementing regulations, and
13 other applicable state and federal privacy and confidentiality laws.

14 (5) "Eligible student" means a student who has reached 18 years of age or is attending an institution of
15 postsecondary education.

16 (6) "FERPA" means the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and its
17 implementing regulations, 34 C.F.R. part 99.3, as amended.

18 (7) "Geolocation data" means information that is, in whole or part, generated by, derived from, or
19 obtained by the operation of an electronic device that can be used to identify the past, present, or future location
20 of an electronic device, an individual, or both.

21 (8) "Internet" means, collectively, the myriad of computer and telecommunications facilities, including

22 equipment and operating software, which comprise the interconnected world-wide network of networks that
23 employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such
24 protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

25 (9) “Internet service” means any service, system, website, application, or program, or portion thereof,
26 including mobile applications and cloud computing services, which accesses the Internet or provides a user with
27 access to the Internet.

28 (10) “K-12 school purposes” means purposes that customarily take place at the direction of a school,
29 teacher, or school district or aid in the administration of school activities, including, but not limited to,
30 instruction in the classroom or at home, administrative activities, preparing for postsecondary education or
31 employment opportunities, and collaboration between students, school personnel, or parents, or are for the use
32 and benefit of the school.

33 (11) “Law enforcement entity” means any government agency or any subunit thereof which performs
34 the administration of criminal justice pursuant to statute or executive order, and which allocates a substantial
35 part of its annual budget to the administration of criminal justice, including but not limited to the Delaware
36 State Police, all law-enforcement agencies and police departments of any political subdivision of this State, the
37 Department of Correction, and the Department of Justice.

38 (12) “Online contact information” means an e-mail address or any other substantially similar identifier
39 that permits direct contact with an individual online, including but not limited to an instant messaging user
40 identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

41 (13) “Operator” means any person other than the Department, school districts, or schools, to the extent
42 that the person:

43 a. Operates an Internet service with actual knowledge that Internet service is used for K-12 school
44 purposes and was designed and marketed for K-12 school purposes; and

45 b. Collects, maintains, or uses student data in a digital or electronic format.

46 (14) “Provisional student data” means new student data proposed for inclusion in the state data system.

47 (15) “School” means any public or private school in the State providing educational instruction in one
48 or more grades from kindergarten through grade 12.

49 (16) “Secretary” means the Secretary of the Department.

50 (17) “State-assigned student identifier” means the unique student identifier assigned by the State to
51 each student that shall not be and shall not include the social security number of a student in whole or in part.

52 (18) “State data system” means a Department state-wide longitudinal data system which allows for the
53 storage, description, management, and reporting of discrete data elements and bodies of information over time.

54 (19) “Student” means any individual attending a school in the State.

55 (20) “Student data” means any information regarding a student that meets any of the following:

56 a. Data descriptive of a student in any media or format, including:

57 i. Student personally identifiable information;

58 ii. State, local, school, or teacher administered assessment results, including participation
59 information;

60 iii. Transcript information including but not limited to courses taken and completed, course
61 grades and grade point average, credits earned, degree, diploma, credential attainment, or other school
62 exit information;

63 iv. Attendance and mobility information between and within local school systems in the State;

64 v. The student’s race, ethnicity, gender, or gender identity;

65 vi. Program participation information required by state or federal law;

66 vii. Disability status;

67 viii. Socioeconomic information;

68 ix. Food purchases; or

69 x. E-mails, text messages, instant messages, documents, search activity, photos, voice
70 recordings; or

71 b. Such information that:

72 i. Is created or provided by a student, or the student’s parent or legal guardian, to an employee
73 or agent of the school district, charter school, or the Department;

74 ii. Is created or provided by a student, or the student’s parent or legal guardian, to an operator
75 in the course of the student’s or parent’s or legal guardian’s use of the operator’s Internet service for
76 K-12 school purposes;

77 ii. Is created or provided by an employee or agent of the school district or school, to an

78 operator; or
79 iii. Is gathered by an operator through the operation of an operator's Internet service for K-12
80 school purposes.

81 (21) "Student personally identifiable information" means any information about a student that,
82 individually or in combination with other information, can be used to distinguish or trace the identity of the
83 student, or information that is linked to information that can be used to distinguish or trace the identity of the
84 student, including the student's name (in whole or in part), signature, physical characteristics or description,
85 residential, school, or other physical address, telephone number, online contact information, social security
86 number, passport number, student identification number, driver's license number, state identification card
87 number, alien registration number, insurance policy number, education history, employment history, bank
88 account number, credit card number, debit card number, or any other financial information, geolocation data,
89 DNA or other genetic material, medical information, or health insurance information, except that it does not
90 include information that is publicly available that is lawfully made available to the general public from federal,
91 state, or local government records.

92 (22) "Targeted advertising" means presenting advertisements to a student, or a student's parent or legal
93 guardian, where the advertisement is selected based on information obtained or inferred from that student's
94 online behavior, usage of applications, or student data. "Targeted advertising" does not include advertising to a
95 student at an online location based upon that student's current visit to that location without collection and
96 retention of a student's online activities over time.

97 **(b) Confidentiality of education records.** ~~Educational Education~~ records of students in all public and private
98 schools in this State are deemed to be confidential. ~~Educational Education~~ records may be released, and student
99 personally identifiable information contained therein disclosed, only in accordance with ~~rules and regulations of the~~
100 ~~Department of Education~~ the provisions of this section and other applicable state and federal law. ~~Such rules and~~
101 ~~regulations shall authorize the release of educational records upon written consent and shall establish the other terms~~
102 ~~and conditions on which educational records may and must be released.~~

103 **(c) Privacy and security of student data; Department responsibilities.** The Department shall promulgate
104 rules and regulations relating to the privacy and protection of student data, and shall be responsible for ensuring
105 compliance with this section and with other state and federal data privacy and security laws by the Department,

106 school districts, and schools, including by doing the following:

107 (1) Establishing Department-wide policies necessary to assure that the use of technologies sustains,
108 enhances, and does not erode privacy protections relating to the use, collection, and disclosure of student data;

109 (2) Maintaining and accessing all records, reports, audits, reviews, documents, papers,
110 recommendations, and other materials available to the Department that relate to programs and operations with
111 respect to the responsibilities of the Department under this section;

112 (3) Ensuring that student data contained in the state data system is handled in full compliance with this
113 section, FERPA, and other state and federal data privacy and security laws;

114 (4) Evaluating legislative and regulatory proposals involving use, collection, and disclosure of student
115 data by the Department;

116 (5) Conducting a privacy impact assessment on legislative proposals, regulations, and program
117 initiatives of the Department, including the type of personal information collected and the number of students
118 affected;

119 (6) Making such investigations and reports relating to the administration of the programs and
120 operations of the Department as are necessary or desirable;

121 (7) Coordinating with the Department of Justice and other legal entities as necessary to ensure that
122 state programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are
123 addressed in an integrated and comprehensive manner;

124 (8) Preparing an annual report to the General Assembly on activities of the Department that affect
125 privacy, including complaints of privacy violations, internal controls, and other matters;

126 (9) Working with the Attorney General and other officials in engaging with stakeholders about the
127 quality, usefulness, openness, and privacy of data;

128 (10) In matters relating to compliance with federal laws, referring the matter to the appropriate federal
129 agency and cooperate with any investigations by such federal agency

130 (11) Establishing and operating a Department-wide Privacy Incident Response Program to ensure that
131 incidents involving Department data are properly reported, investigated, and mitigated, as appropriate;

132 (12) Establishing a model process and policy for parents and eligible students to file complaints of
133 privacy violations or inability to access their children's or their education records against the school district or

134 school; and

135 (13) Providing training, guidance, technical assistance, and outreach to build a culture of privacy
136 protection, data security, and data practice transparency to students, parents, and the public among all state and
137 local governmental education entities that collect, maintain, use, or share student data.

138 (d) *State data system and student personally identifiable information; Department responsibilities.* The
139 Department shall:

140 (1) Create, publish, and make publicly available a data inventory and dictionary or index of data
141 elements with definitions of student personally identifiable information fields in the state data system to include,
142 but not be limited to:

143 a. Any student personally identifiable information required to be reported by state and federal
144 education mandates;

145 b. Any student personally identifiable information which is included or has been proposed for
146 inclusion in the state data system with a statement regarding the purpose or reason for the proposed
147 collection; and

148 c. Any student data that the Department collects or maintains with no current identified purpose;

149 (2) Promulgate rules and regulations for the state data system to comply with this article and other
150 applicable state and federal data privacy and security laws, including FERPA. Such rules and regulations shall
151 include, at a minimum:

152 a. Restrictions on granting access to student data in the state data system, except to the following:

153 i. Students and their parents, as provided by the collecting school district or school;

154 ii. Authorized administrators, teachers, and other personnel of school districts or schools, and
155 contractors or other authorized persons working on their behalf, that enroll students who are the subject
156 of the data and who require such access to perform their assigned duties;

157 iii. Authorized staff of the Department, and contractors or other authorized persons working
158 on behalf of the Department, who require such access to perform their assigned duties as authorized by
159 law or defined by interagency or other data-sharing agreements; and

160 iv. Authorized staff of other State agencies as required or authorized by law, including
161 contractors or other authorized persons working on behalf of a state agency that require such access to

- 162 perform their duties pursuant to an interagency agreement or other data-sharing agreement;
- 163 b. Prohibitions against publishing student data other than as specifically permitted herein; and
- 164 c. Consistent with applicable law, criteria for the approval of research and data requests from state
- 165 and local agencies, the General Assembly, persons conducting research including on behalf of the
- 166 Department, and the public that involve access to student personally identifiable information;
- 167 (3) Unless otherwise provided by law or approved by the Department, not transfer student personally
- 168 identifiable information to any state, federal, or local agency or nongovernmental organization, except for
- 169 disclosures incident to the following actions:
- 170 a. A student transferring to another school or school system in this State or out of state or a school
- 171 or school system seeking help with locating a transferred student;
- 172 b. A student enrolling in a postsecondary institution or training program;
- 173 c. A student registering for or taking a state, national, or multistate assessment where such data is
- 174 required to administer the assessment;
- 175 d. A student voluntarily participating in a program for which such a data transfer is a condition or
- 176 requirement of participation;
- 177 e. The federal government requiring the transfer of student data for a student classified as a
- 178 “migrant” for related federal program purposes;
- 179 f. A federal agency requiring student personally identifiable information to perform an audit,
- 180 compliance review, or complaint investigation; or
- 181 g. An eligible student or student’s parent or legal guardian requesting such transfer;
- 182 (4) Develop a detailed data security plan for the state data system that includes:
- 183 a. Guidelines for authorizing access to the state data system and to student personally identifiable
- 184 information including guidelines for authentication of authorized access;
- 185 b. Privacy and security audits;
- 186 c. Plans for responding to security breaches, including notifications, remediations, and related
- 187 procedures;
- 188 d. Data retention and disposal policies;
- 189 e. Data security training and policies including technical, physical, and administrative safeguards;

190 f. Standards regarding the minimum number of students or information that must be included in a
191 data set in order for the data to be considered aggregated and, therefore, not student personally identifiable
192 information subject to requirements in this article and in other federal and state data privacy laws;

193 g. A process for evaluating and updating as necessary the data security plan, at least on an annual
194 basis, in order to identify and address any risks to the security of student personally identifiable
195 information; and

196 h. Guidance for local boards of education to implement effective security practices that are
197 consistent with those of the state data system;

198 (5) Ensure routine and ongoing compliance by the Department with FERPA, other relevant privacy
199 laws and policies, and the privacy and security rules and regulations promulgated under the authority of this
200 section, including the performance of compliance audits for the Department;

201 (6) Notify the Governor and the General Assembly annually of the following matters relating to the
202 state data system:

203 a. New provisional student data proposed for inclusion in the state data system:

204 i. Any new provisional student data collection proposed by the Department shall become a
205 provisional requirement to allow local boards of education and their local data system vendors the
206 opportunity to meet the new requirement; and

207 ii. The Department shall announce any new provisional student data collection to the general
208 public for a review and comment period of at least 60 days;

209 b. Changes to existing student personally identifiable information collections required for any
210 reason, including changes to federal reporting requirements made by the United States Department of
211 Education;

212 c. A list of any special approvals granted by the Department pursuant to paragraph (3)c. of
213 subsection (d) of this section in the past year regarding the release of student personally identifiable
214 information; and

215 d. The results of any and all privacy compliance and security audits completed in the past year.
216 Notifications regarding privacy compliance and security audits shall not include any information that would
217 itself pose a security threat to the state or local student information systems or to the secure transmission of

218 data between state and local systems by exposing vulnerabilities; and

219 (7) Promulgate rules and regulations to ensure the provision of at least annual notifications to eligible
220 students and parents or guardians regarding student privacy rights under state and federal law.

221 (e) Restrictions on reporting student data. Unless required by state or federal law or in cases of health or
222 safety emergencies, school districts and schools shall not report to the Department the following student data:

223 (1) Juvenile delinquency records;

224 (2) Criminal records; or

225 (3) Medical and health records.

226 (f) Restrictions on collecting certain data on students or their families. Unless required by state or federal
227 law or in cases of health or safety emergencies, school districts and schools shall not collect the following data on
228 students or their families:

229 (1) Political affiliation;

230 (2) Voting history;

231 (3) Income, except as required by law or where a school district or school determines income
232 information is required to apply for, administer, research, or evaluate programs to assist students from low-
233 income families; or

234 (4) Religious affiliation or beliefs.

235 (g) Operators; duties. An operator shall:

236 (1) Implement and maintain reasonable security procedures and practices appropriate to the nature of
237 the student data to protect that information from unauthorized access, destruction, use, modification, or
238 disclosure; and

239 (2) Delete a student's data within a reasonable timeframe not to exceed 45 days if the school district or
240 school requests deletion of data under the control of the school district or school.

241 (h) Operators; prohibited activities. An operator shall not knowingly engage in any of the following
242 activities with respect to such operator's Internet service:

243 (1) Engage in targeted advertising on the operator's Internet service, or on any other Internet service,
244 when the targeting of the advertising is based upon any information, including student data and state-assigned
245 student identifiers or other persistent unique identifiers, that the operator has acquired because of the use of an

246 Internet service as described in paragraph (13) of subsection (a) of this section:

247 (2) Use information, including state-assigned student identifiers or other persistent unique identifiers,
248 created or gathered by an Internet service as described in paragraph (13) of subsection (a) of this section, to
249 amass a profile about a student except in furtherance of K-12 school purposes;

250 (3) Sell a student's student data. This prohibition does not apply to the purchase, merger, or other type
251 of acquisition of an operator by another entity, provided that the operator or successor entity continues to be
252 subject to the provisions of this section with respect to previously-acquired student data that is subject to this
253 section; or

254 (4) Disclose student data, unless the disclosure is made:

255 a. In furtherance of the K-12 school purposes of the Internet service; provided that the recipient of
256 the student data disclosed (i) shall not further disclose the student data unless done to allow or improve the
257 operability and functionality within that student's classroom or school, and (ii) is legally required to
258 comply with the requirements of subsection (g) of this section or paragraphs (1) through (3) of this
259 subsection;

260 b. To ensure legal or regulatory compliance;

261 c. To respond to or participate in judicial process;

262 d. To protect the security or integrity of the operator's Internet service;

263 e. To protect the safety of users or others or security of the Internet service; or

264 f. To a service provider, provided that the operator contractually (i) prohibits the service provider
265 from using any student data for any purpose other than providing the contracted service to, or on behalf of,
266 the operator, (ii) prohibits the service provider from disclosing to subsequent third parties any student data
267 provided by the operator, and (iii) requires the service provider to comply with the requirements of
268 paragraphs (1) through (3) of this subsection and to implement and maintain reasonable security procedures
269 and practices as provided in paragraph (1) of subsection (g) of this section.

270 (5) Notwithstanding paragraph (4) of this subsection, an operator may disclose student data under the
271 following circumstances, so long as paragraphs (1) to (3), inclusive, of this subsection are not violated:

272 a. If another provision of state or federal law requires the operator to disclose the student data, and
273 the operator complies with the requirements of applicable state and federal law in protecting and disclosing

274 that information:

275 b. For legitimate research purposes:

276 i. As required by state or federal law and subject to the restrictions under applicable state or
277 federal law; or

278 ii. As allowed by state or federal law and under the direction of a school district, school, or the
279 Department, if no student data is used for any purpose in furtherance of advertising or to amass a
280 profile on the student for purposes other than K-12 school purposes; or

281 c. To a state agency, school district, or school, for K-12 school purposes, as permitted by state or
282 federal law.

283 (6) Nothing in this subsection prohibits an operator from using student data as follows:

284 a. For maintaining, delivering, supporting, evaluating, or diagnosing the operator's Internet
285 service; or

286 b. For adaptive learning or customized student learning purposes.

287 (7) Nothing in this subsection prohibits an operator from using or sharing aggregate student data or de-
288 identified student data as follows:

289 a. For the development and improvement of the operator's Internet service or other educational
290 Internet services;

291 b. Within other Internet services owned by the operator, and intended for school district, school, or
292 student use, to evaluate and improve educational products or services intended for school district, school, or
293 student use; or

294 c. To demonstrate the effectiveness of the operator's products or services, including their
295 marketing.

296 (i) Exclusions. This section shall not be construed so as to do any of the following:

297 (1) Apply to general audience Internet services, even if login credentials created for an operator's
298 Internet service may be used to access those general audience Internet services;

299 (2) Limit the authority of a law enforcement agency to obtain any content or student data from an
300 operator as authorized by law or pursuant to an order of a court of competent jurisdiction;

301 (3) Limit Internet service providers from providing Internet connectivity to schools or students and

302 their families;

303 (4) Prohibit an operator from marketing educational products directly to parents, so long as the
304 marketing does not result from the use of student data obtained by the operator through the provision of services
305 covered under this section;

306 (5) Impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of
307 purchasing or downloading software or applications to review or enforce compliance with this section on those
308 applications or software;

309 (6) Impose a duty upon a provider of an interactive computer service, as defined in § 230 of Title 47 of
310 the United States Code, to review or enforce compliance with this section by third-party content providers;

311 (7) Impede the ability of a student or parent or guardian to download, transfer, export, or otherwise
312 save or maintain their own student data or documents; or

313 (8) Prevent the Department, school district, or school from recommending, solely for K-12 school
314 purposes, any educational materials, online content, services, or other products to any student or to the student's
315 family if the Department, school district, or school determines that such products will benefit the student and no
316 person receives compensation for developing, enabling, or communicating such recommendations.

317 ~~(b)(j)~~ The provisions of subsection (a) subsections (e) through (h) of this section notwithstanding,
318 educational institutions and programs operating in this State, including postsecondary institutions and programs
319 regulated by a state agency, shall disclose to the Department such education records, and student personally
320 identifiable information contained therein, necessary for the audit or evaluation of state and federal education
321 programs in accordance with the terms and conditions of a written agreement negotiated between the Department
322 and each educational institution or program from which education records are sought. Such agreements shall:

323 (1) State the term of the agreement;

324 (2) Comply with the requirements of ~~the Family Educational Rights and Privacy Act Regulations set~~
325 ~~forth in 34 CFR Part 99~~ FERPA regarding the Department's use, compilation, maintenance, protection,
326 distribution, re-disclosure and return/destruction of education records obtained hereunder;

327 (3) Specify the data elements to be disclosed by the educational institution or program;

328 (4) State the purpose for which the information will be used;

329 (5) Prohibit any disclosure of education records or student personally identifiable information

330 contained therein by an educational institution or program in violation of applicable state or federal privacy
331 laws;

332 (6) Prohibit any modification or amendment except by written agreement duly executed by the parties;
333 and

334 (7) Contain such additional provisions as agreed upon.

335 All disclosures required by this subsection shall be for the purpose of ensuring the effectiveness of publicly-
336 funded programs by connecting pre-kindergarten through grade 12 and post-secondary data, and sharing
337 information to improve early childhood and workforce programs as set forth in Delaware's State Fiscal
338 Stabilization Plan and Delaware's Race to the Top Plan, or as otherwise approved by the P-20 Council.

339 ~~(e)~~(k) *Inspection and review of education records.*

340 (1) All public and private school districts and schools in this State shall allow parents and eligible
341 students to inspect and review the education records of their children or themselves who are, or have been, in
342 attendance at the school. The right to inspect and review educational education records shall be in accordance
343 with this subsection and rules and regulations of promulgated by the Department.

344 (2) Parents or legal guardians, and eligible students, may request from the school district or school
345 student data included in the student's education record, including student data maintained by an operator, except
346 when the school district or school determines that the requested data maintained by the operator cannot
347 reasonably be made available to the parent.

348 (3) School districts or charter schools shall provide parents or legal guardians, and eligible students,
349 with an electronic copy of their children's or their own education record upon request, unless the school district
350 or school does not maintain a record in electronic format and reproducing the record in an electronic format
351 would be unduly burdensome.

352 (4) A parent or eligible student shall have the right to request corrections to inaccurate education
353 records maintained by a school district or school. After receiving a request demonstrating any such inaccuracy,
354 the school district or school that maintains the data shall correct the inaccuracy and confirm such correction to
355 the parent or legal guardians, or eligible student, within a reasonable amount of time.

356 (5) The Department shall promulgate rules and regulations that:

357 a. Support school districts and schools in fulfilling their responsibility to annually notify parents or

358 legal guardians and eligible students of their right to request student data;

359 b. Assist school districts and schools with ensuring security when providing student data to parents
360 or legal guardians and eligible students;

361 c. Provide guidance and best practices to school districts and schools in order to ensure that school
362 districts and schools provide student data only to authorized individuals;

363 d. Support school districts and schools in their responsibility to produce education records and
364 student data included in such education records to parents or legal guardians and eligible students, ideally
365 within three business days of the request;

366 e. Assist school districts and schools with implementing technologies and programs that allow
367 parents or legal guardians and eligible students to view online, download, and transmit data specific to their
368 children's or their own education record.

369 f. Enable parents or legal guardians, or eligible students to file a complaint with a school district or
370 school regarding a possible violation of rights under this section or under other state or federal student data
371 privacy and security laws which shall ensure that:

372 i. Each school district or school designates at least one individual with responsibility to
373 address complaints filed by parents or legal guardians, or eligible students;

374 ii. The individual designated by the school district or school shall provide a written decision
375 in response to the parent's or legal guardian's or eligible student's complaint; and

376 iii. A party dissatisfied with the decision may appeal it, first to the superintendent or person of
377 similar position in the school district or school, then, if further appeal is sought, to the board of
378 education or other governing body of the school district or school, and, finally, if further appeal is
379 sought, to the State Board of Education.

380 ~~(4)(l)~~ No cause of action or claim for relief, civil or criminal, shall lie or damages be recoverable against
381 any school officer or employee by reason of such officer's or employee's participation in the formulation of such
382 education records or any statements made or of judgments expressed therein concerning a student's academic
383 performance, personal conduct, health, habits, school related activities or potential; nor by reason of the disclosure
384 of the education records or personally identifiable information from student data contained within the education
385 records, nor lack of access thereto, in accordance with subsections (a) through (e) of a manner authorized or

386 permitted by this section.

387 Section 2. This Act becomes effective on August 1 following its enactment into law.

388 Section 3. The provisions of this Act do not apply to projects relating to the privacy and security of student
389 data approved prior to the effective date of this Act under the Department of Education’s existing data governance
390 regulation, Regulation 294 of Title 14 of the Delaware Administrative Code.

391 Section 4. This Act shall be known and may be cited as the “Student Data Privacy Protection Act.”

SYNOPSIS

This bill amends Section 4111 of Title 14 of the Delaware Code to establish policies and procedures that enable school districts, schools, teachers, and school staff to collect and use student data for appropriate educational purposes while ensuring that the student data is kept safe and the privacy of students and their parents and guardians is protected.

The bill provides that the Department of Education shall be responsible developing policies and procedures relating to the privacy and protection of student data in accordance with the act, and shall be responsible for ensuring compliance with the act’s provisions and with other state and federal data privacy and security laws by the Department, school districts, and schools, including by undertaking certain specified activities.

The bill also establishes the duties and responsibilities of operators of Internet services used for school purposes with respect to student data they collect, including student personally identifiable information.

Further, the bill recognizes the right of parents and eligible students to review and obtain copies of their children’s or their own education records and to request the correction of information in the education records which is incorrect or false.

Finally, the bill provides that its provisions will become effective on August 1 the year following its enactment into law, and that its provisions do not apply to projects relating to the privacy and security of student data approved under the Department of Education’s existing education record privacy regulation prior to the effective date of the Act.

Author: Senator Sokola