

WEST VIRGINIA LEGISLATURE

2016 REGULAR SESSION

ENROLLED

Committee Substitute

for

House Bill 4261

BY DELEGATES SHOTT, MCCUSKEY, COWLES, O'NEAL,

BUTLER, MARCUM, SHAFFER, SOBONYA, FOLK,

OVERINGTON AND AZINGER

[Passed March 12, 2016; in effect ninety days from
passage.]

1 AN ACT to amend and reenact §18-2-5h of the Code of West Virginia, 1931, as amended, relating
2 to student data; prohibiting the West Virginia Department of Education from transferring
3 confidential student information or certain redacted data to any federal, state or local
4 agency or other person or entity; establishing exception when the department enters into
5 a contract that governs student or redacted data with a contractor for the purposes of state
6 level reporting; establishing exception that, in the event the ACT or the SAT tests are

7 adopted as the state summative assessment, allows the ACT or the College Board to use
8 a certain information; requiring written consent if information classified as confidential is
9 required; and requiring consent contain a detailed list of confidential information required
10 and the purpose of its requirement.

Be it enacted by the Legislature of West Virginia:

1 That §18-2-5h of the Code of West Virginia, 1931, as amended, be amended and
2 reenacted to read as follows:

ARTICLE 2. STATE BOARD OF EDUCATION.

§18-2-5h. Student Data Accessibility, Transparency and Accountability Act.

1 (a) *Title.* — This section shall be known and may be cited as the “Student Data
2 Accessibility, Transparency and Account-ability Act.”

3 (b) *Definitions.* — As used in this section, the following words have the meanings ascribed
4 to them unless the context clearly implies a different meaning:

5 (1) “Board” means the West Virginia Board of Education;

6 (2) “Department” means the West Virginia Department of Education;

7 (3) “Student Data system” means the West Virginia Department of Education statewide
8 longitudinal data system;

9 (4) “Aggregate data” means data collected that is reported at the group, cohort, or
10 institutional level with a data set of sufficient size that no information for an individual parent or
11 student is identifiable;

12 (5) “Redacted data” means a student dataset in which parent and student identifying
13 information has been removed;

14 (6) “State-assigned student identifier” means the unique student identifier assigned by the
15 state to each student that shall not be or include the Social Security number of a student in whole
16 or in part;

17 (7) “Student data” means data collected or reported at the individual student level included

18 in a student's educational record;

19 (8) "Provisional student data" means new student data proposed for inclusion in the
20 student data system;

21 (9) "School district" means a county board of education, the West Virginia Schools for the
22 Deaf and Blind and the West Virginia Department of Education with respect to the education
23 programs under its jurisdiction that are not in the public schools;

24 (10) "Directory information" means the following individual student information that is
25 subject to disclosure for school-related purposes only: Student name, address, telephone
26 number, date and place of birth, major field of study, participation in officially recognized activities
27 and sports, weight and height of members of athletic teams, dates of attendance, indication of
28 "graduate" or "nongraduate," degrees and awards receives, most recent previous school
29 attended, and photograph.

30 (11) "Confidential student information" means data relating to a person's Social Security
31 number, or other identification number issued by a state or federal agency, except for the state-
32 assigned student identifier as defined in this section, religious affiliation, whether the person or a
33 member of their household owns or possesses a firearm, whether the person or their family are
34 or were recipients of financial assistance from a state or federal agency, medical, psychological
35 or behavioral diagnoses, criminal history, criminal history of parents, siblings or any members of
36 the person's household, vehicle registration number, driver's license number, biometric
37 information, handwriting sample, credit card numbers, consumer credit history, credit score, or
38 genetic information;

39 (12) "Affective computing" means human-computer interaction in which the device has the
40 ability to detect and appropriately respond to its user's emotions and other stimuli; and

41 (13) "Fair Information Practice Principles" are United States Federal Trade Commission
42 guidelines that represent widely accepted concepts concerning fair information practice in an

43 electronic marketplace.

44 (c) *Data Inventory – State Responsibilities.* – The Department of Education shall:

45 (1) Create, publish, and make publicly available a data inventory and dictionary or index
46 of data elements with definitions of individual student data fields in the student data system to
47 include, but not be limited to:

48 (A) Any individual student data required to be reported by state and federal education
49 mandates;

50 (B) Any individual student data which has been proposed in accordance with paragraph
51 (A), subdivision (7) of this subsection for inclusion in the student data system with a statement
52 regarding the purpose or reason and legal authority for the proposed collection; and

53 (C) Any individual student data that the department collects or maintains with no current
54 identified purpose;

55 (2) Develop, publish, and make publicly available policies and procedures to comply with
56 all relevant state and federal privacy laws and policies, including, but not limited to, the Federal
57 Family Educational Rights and Privacy Act (FERPA) and other relevant privacy laws and policies.
58 The policies and procedures specifically shall include, but are not limited to:

59 (A) Access to student and redacted data in the statewide longitudinal data system shall
60 be restricted to:

61 (i) The authorized staff of the department and the contractors working on behalf of the
62 department who require access to perform their assigned duties as required by law and defined
63 by interagency data-sharing agreements;

64 (ii) District administrators, teachers and school personnel who require access to perform
65 their assigned duties;

66 (iii) Students and their parents; and

67 (iv) The authorized staff of other West Virginia state agencies as required by law and

68 defined by interagency data-sharing agreements;

69 (B) Ensure that any inter-agency data-sharing agreements shall be posted on the
70 Department website, and parents shall be notified of their right to opt out of sharing the child's
71 data pursuant to agreements.

72 (C) Use only aggregate data in public reports or in response to record requests in
73 accordance with this section;

74 (D) Unless otherwise prohibited by law, develop criteria for the approval of research and
75 data requests from state and local agencies, the Legislature, researchers working on behalf of
76 the department, and the public. Student data maintained by the department shall remain redacted;
77 and

78 (E) Notification to students and parents regarding student privacy rights under federal and
79 state law;

80 (3) Unless otherwise provided by law, the department shall not transfer confidential
81 student information or redacted data that is confidential under this section to any federal, state or
82 local agency or other person or entity, public or private, with the following exceptions:

83 (A) A student transfers out-of-state or a school or school district seeks help with locating
84 an out-of-state transfer;

85 (B) A student leaves the state to attend an out-of-state institution of higher education or
86 training program;

87 (C) A student registers for or takes a national or multistate assessment;

88 (D) A student voluntarily participates in a program for which a data transfer is a condition
89 or requirement of participation;

90 (E) The department enters into a contract that governs databases, assessments, student
91 or redacted data, special education or instructional supports with an in-state or out-of-state
92 contractor for the purposes of state level reporting;

93 (F) A student is classified as “migrant” for federal reporting purposes;

94 (G) A federal agency is performing a compliance review; or

95 (H) In the event that the ACT or the SAT tests are adopted for use as the state summative
96 assessment, nothing in this article prevents the ACT or the College Board from using a student’s
97 assessment results and necessary directory or other permissible information under this Act. If
98 information classified as confidential is required, the ACT, SAT or College Board shall obtain
99 affirmative written consent from the student if the student is eighteen years of age or older, or
100 from the student’s parent or guardian if the student is under eighteen years of age. The consent
101 shall contain a detailed list of confidential information required and the purpose of its requirement.

102 (4) Develop a detailed data security plan that includes:

103 (A) Guidelines for the student data system and for individual student data including
104 guidelines for authentication of authorized access;

105 (B) Privacy compliance standards;

106 (C) Privacy and security audits;

107 (D) Breach planning, notification and procedures;

108 (E) Data retention and disposition policies; and

109 (F) Data security policies including electronic, physical, and administrative safeguards,
110 such as data encryption and training of employees;

111 (5) Ensure routine and ongoing compliance by the department with FERPA, other relevant
112 privacy laws and policies, and the privacy and security policies and procedures developed under
113 the authority of this act, including the performance of compliance audits;

114 (6) Ensure that any contracts that govern databases, assessments or instructional
115 supports that include student or redacted data and are outsourced to private vendors include
116 express provisions that safeguard privacy and security and include penalties for noncompliance;
117 and

118 (7) Notify the Governor and the Legislature annually of the following:

119 (A) New student data proposed for inclusion in the state student data system. Any proposal
120 by the Department of Education to collect new student data must include a statement regarding
121 the purpose or reason and legal authority for the proposed collection. The proposal shall be
122 announced to the general public for a review and comment period of at least sixty days and
123 approved by the state board before it becomes effective. Any new student data collection
124 approved by the state board is a provisional requirement for a period sufficient to allow schools
125 and school districts the opportunity to meet the new requirement;

126 (B) Changes to existing data collections required for any reason, including changes to
127 federal reporting requirements made by the U.S. Department of Education and a statement of the
128 reasons the changes were necessary;

129 (C) An explanation of any exceptions granted by the state board in the past year regarding
130 the release or out-of-state transfer of student or redacted data; and

131 (D) The results of any and all privacy compliance and security audits completed in the past
132 year. Notifications regarding privacy compliance and security audits shall not include any
133 information that would itself pose a security threat to the state or local student information systems
134 or to the secure transmission of data between state and local systems by exposing vulnerabilities.

135 (8) Notify the Governor upon the suspicion of a data security breach or confirmed breach
136 and upon regular intervals as the breach is being managed. The parents shall be notified as soon
137 as possible after the suspected or confirmed breach.

138 (9) Prohibit the collection of confidential student information as defined in subdivision ten
139 of subsection (b) of this section.

140 (d) *Data Inventory - District Responsibilities.* — A school district shall not report to the state
141 the following individual student data:

142 (1) Juvenile delinquency records;

143 (2) Criminal records;

144 (3) Medical and health records; and

145 (4) Student biometric information.

146 (e) *Data Inventory – School Responsibilities.* – Schools shall not collect the following
147 individual student data:

148 (1) Political affiliation and beliefs;

149 (2) Religion and religious beliefs and affiliations;

150 (3) Any data collected through affective computing;

151 (4) Any data concerning the sexual orientation or beliefs about sexual orientation of the
152 student or any student’s family member; and

153 (5) Any data concerning firearm’s ownership by any member of a student’s family.

154 (f) *Data Governance Manager.* – The state superintendent shall appoint a data
155 governance manager, who shall report to and be under the general supervision of the state
156 superintendent. The data governance manager shall have primary responsibility for privacy policy,
157 including:

158 (1) Assuring that the use of technologies sustain, and do not erode, privacy protections
159 relating to the use, collection, and disclosure of student data;

160 (2) Assuring that student data contained in the student data system is handled in full
161 compliance with the Student Data Accessibility, Transparency, and Accountability Act, FERPA,
162 and other state and federal privacy laws;

163 (3) Evaluating legislative and regulatory proposals involving collection, use, and disclosure
164 of student data by the Department of Education;

165 (4) Conducting a privacy impact assessment on proposed rules of the state board and
166 department in general and on the privacy of student data, including the type of personal
167 information collected and the number of students affected;

168 (5) Coordinating with the general counsel of the state board and department, other legal
169 entities, and organization officers to ensure that programs, policies, and procedures involving civil
170 rights, civil liberties, and privacy considerations are addressed in an integrated and
171 comprehensive manner;

172 (6) Preparing a report to the Legislature on an annual basis on activities of the department
173 that affect privacy, including complaints of privacy violations, internal controls, and other matters;

174 (7) Establishing department-wide policies necessary for implementing Fair Information
175 Practice Principles to enhance privacy protections;

176 (8) Working with the Office of Data Management and Analysis, the general counsel, and
177 other officials in engaging with stakeholders about the quality, usefulness, openness, and privacy
178 of data;

179 (9) Establishing and operating a department-wide Privacy Incident Response Program to
180 ensure that incidents are properly reported, investigated and mitigated, as appropriate;

181 (10) Establishing and operating a process for parents to file complaints of privacy
182 violations;

183 (11) Establishing and operating a process to collect and respond to complaints of privacy
184 violations and provides redress, as appropriate; and

185 (12) Providing training, education and outreach to build a culture of privacy across the
186 department and transparency to the public.

187 The data governance manager shall have access to all records, reports, audits, reviews,
188 documents, papers, recommendations, and other materials available to the department that relate
189 to programs and operations with respect to his or her responsibilities under this section and shall
190 make investigations and reports relating to the administration of the programs and operations of
191 the department as are necessary or desirable.

192 (g) *Parental rights regarding child's information and education record.* — Parents have the

193 right to inspect and review their child's education record maintained by the school and to request
194 student data specific to their child's educational record. School districts must provide parents or
195 guardians with a copy of their child's educational record upon request. Whenever possible, an
196 electronic copy of the educational record must be provided if requested and the identity of the
197 person requesting the information is verified as the parent or guardian.

198 The state board shall develop guidance for school district policies that:

199 (1) Annually notify parents of their right to request student information;

200 (2) Ensure security when providing student data to parents;

201 (3) Ensure student data is provided only to the authorized individuals;

202 (4) Detail the timeframe within which record requests must be provided;

203 (5) Ensure that school districts have a plan to allow parents to view and access data
204 specific to their child's educational record and that any electronic access provided is restricted to
205 eligible parties;

206 (6) Ensure compliance in the collection, use and disclosure of directory information and
207 providing parents or guardians with a form to limit the information concerning their child in
208 directory and subject to release; and

209 (7) Informing parents of their rights and the process for filing complaints of privacy
210 violations.

211 (h) *State Board Rules.* — The state board shall adopt rules necessary to implement the
212 provisions of the Student Data Accessibility, Transparency, and Accountability Act.

213 (i) *Effect on Existing Data.* — Upon the effective date of this section, any existing student
214 data collected by the Department of Education shall not be considered a new student data
215 collection under this section.