

SENATE FILE NO. SF0014

Student data privacy and transparency.

Sponsored by: Joint Education Interim Committee

A BILL

for

1 AN ACT relating to education; prohibiting school districts
 2 from accessing students' digital information accounts as
 3 specified; providing for criminal penalties; amending
 4 requirements of state data security plan to ensure privacy
 5 of student data collected; requiring policies for the
 6 collection, access, security and use of student data by
 7 school districts; accordingly imposing duties; and
 8 providing for an effective date.

9

10 *Be It Enacted by the Legislature of the State of Wyoming:*

11

12 **Section 1.** W.S. 21-3-132 is created to read:

13

14 **21-3-132. Student digital information privacy;**
 15 **prohibited acts; exceptions; penalties.**

16

1 (a) No officer or employee of a school district
2 organized within this state shall:

3

4 (i) Require or request a student or prospective
5 student to disclose or to provide access to a digital
6 information account through the student's or prospective
7 student's username, password or other means of
8 authentication that provides access;

9

10 (ii) Require or request a student or prospective
11 student to access a digital information account in the
12 presence of any officer or employee of the school district
13 in a manner that enables the officer or employee to observe
14 the contents of the digital information account;

15

16 (iii) Compel a student or prospective student to
17 add anyone to the student's or prospective student's list
18 of contacts associated with a digital information account
19 or require, request or cause a student or prospective
20 student to change the privacy settings associated with a
21 digital information account;

22

1 (iv) Expel, discharge, discipline, fail or
2 refuse to admit or otherwise penalize or threaten a student
3 or prospective student for refusing to disclose information
4 or to take action specified in this section;

5

6 (v) Require or request a student or prospective
7 student to waive or limit any protection granted under this
8 section.

9

10 (b) Nothing in this section shall prohibit an officer
11 or employee of a school district from:

12

13 (i) Conducting an investigation, without
14 requiring or requesting access to a digital information
15 account through username, password or other means of
16 authentication, for the purpose of ensuring compliance with
17 applicable law or school policies against student
18 misconduct based on the receipt of specific information
19 about activity associated with a student's digital
20 information account;

21

22 (ii) Requesting or receiving written or
23 electronic consent from a student or prospective student,

1 if emancipated or eighteen (18) years of age or older, or
2 the student's or prospective student's parent or legal
3 guardian if the student or prospective student is an
4 unemancipated minor, to observe the contents of a digital
5 information account, without requiring or requesting access
6 to the account through username, password or other means of
7 authentication;

8

9 (iii) Viewing, accessing or utilizing
10 information about a student or prospective student that is
11 publicly available.

12

13 (c) Nothing in this section shall apply to an account
14 opened, created or provided by a school district if the
15 student has been provided advance notice that the account
16 may be monitored at any time by an officer or employee of
17 the school district.

18

19 (d) This section does not create a duty for an
20 officer or employee of a school district to search or
21 monitor the activity of a student's or prospective
22 student's digital information account.

23

1 (e) Any officer or employee of a school district
2 violating the provisions of this section is guilty of a
3 misdemeanor punishable by a fine of not more than two
4 hundred fifty dollars (\$250.00) for the first violation and
5 one thousand dollars (\$1,000.00) for each subsequent
6 violation.

7

8 (f) For purposes of this section "digital information
9 account" means an electronic service or account used to
10 communicate or store digital assets.

11

12 **Section 2.** W.S. 21-2-202(a)(xxxiv)(intro), (H), (J),
13 by creating new subparagraph (K) and by creating a new
14 paragraph (xxxvii) and 21-3-110(a) by creating new
15 paragraphs (xxxv) and (xxxvi) are amended to read:

16

17 **21-2-202. Duties of the state superintendent.**

18

19 (a) In addition to any other duties assigned by law,
20 the state superintendent shall:

21

22 (xxxiv) With the department of enterprise
23 technology services, establish criteria for the collection,

1 storage, management and reporting of department of
2 education data ~~related~~ including, but not limited to
3 teacher certification, statewide education accountability
4 and assessment and the administration of the school finance
5 system. In carrying out this paragraph, the state
6 superintendent and the department of enterprise technology
7 services shall develop a data security plan that includes:

8

9 (H) Prohibition of the sale or trade of
10 student data to private entities or organizations; ~~and~~

11

12 (J) All personally identifiable student
13 information being reported to the department of education
14 or the department of enterprise technology by a student's
15 Wyoming student record identification and locator number as
16 issued by the department of education; ~~and~~ and

17

18 (K) Standards and protocols to remove
19 personally identifiable information to conduct data
20 collection and analysis without disclosing the identity of
21 the student whose data is being collected and used.

22

1 (xxxvii) In consultation with the department of
2 enterprise technology, the department of audit and school
3 districts, establish and maintain guidelines for school
4 districts for the collection, access, security and use of
5 student data by school districts. The guidelines shall, at
6 a minimum, be in compliance with the federal Family
7 Educational Rights and Privacy Act and other relevant
8 federal and state laws and include the following:

9
10 (A) Authorization and authentication
11 mechanisms for accessing student data;

12
13 (B) Administrative, physical and logical
14 security safeguards, including employee training and data
15 encryption;

16
17 (C) Privacy and security compliance
18 standards;

19
20 (D) Processes for identification of and
21 response to data security incidents, including breach
22 notification and mitigation procedures;

23

1 (E) Standards for retention and destruction
2 of student data.

3

4 **21-3-110. Duties of boards of trustees.**

5

6 (a) The board of trustees in each school district
7 shall:

8

9 (xxxv) Adopt and enforce a policy regarding the
10 collection, access, security and use of student data in
11 accordance with guidelines established by the state
12 superintendent under W.S. 21-2-202(a) (xxxvii);

13

14 (xxxvi) At a minimum, ensure compliance with
15 W.S. 21-3-132.

16

17 **Section 3.** This act is effective July 1, 2016.

18

19

(END)