

**HB**

**257**

<TARGET><BILL>HB 257</BILL><SUBJECT>HB  
257</SUBJECT><COMM>HEDC28</COMM></TARGET>

28-LS1096\Y  
Mischel  
4/10/14

**CS FOR HOUSE BILL NO. 257( )**  
**IN THE LEGISLATURE OF THE STATE OF ALASKA**  
**TWENTY-EIGHTH LEGISLATURE - SECOND SESSION**

**BY**

**Offered:**  
**Referred:**

**Sponsor(s): REPRESENTATIVE REINBOLD**

**A BILL**  
**FOR AN ACT ENTITLED**

1 **"An Act relating to restrictions on the collection, storage, and handling of student data."**

2 **BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:**

3 **\* Section 1.** AS 14.03.115 is amended to read:

4 **Sec. 14.03.115. Access to school records [BY PARENT, FOSTER**  
5 **PARENT, OR GUARDIAN].** Upon request of a parent, foster parent, or guardian of  
6 a child under 18 years of age who is currently or was previously enrolled in a  
7 municipal school district or a school district that is a regional educational attendance  
8 area, the school district shall provide a written or electronic copy of the child's  
9 record, including student data, based on the preference of the parent, foster  
10 parent, or guardian. This section does not apply to

- 11 (1) a record of a child who is an emancipated minor; or
- 12 (2) record information that consists of the child's address if the school
- 13 district determines that the release of the child's address poses a threat to the health or
- 14 safety of the child.

15 **\* Sec. 2.** AS 14.03.115 is amended by adding a new subsection to read:

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31

(b) A school, a district, or the department may use student data that contains personally identifiable information for a commercial purpose only by first obtaining written consent, within six months of the use, from the student's parent or legal guardian or from the student if the student is 18 years of age or older or is emancipated under AS 09.55.590. Consent must be dated when signed and state the limited purpose for which the consent is provided and the records that may be used. In this subsection, "commercial purpose" includes marketing of products or services, compilation of lists for sale or rent, development of products or services, and the creation of individual, household, or group profiles.

\* **Sec. 3.** AS 14.03 is amended by adding a new section to read:

**Sec. 14.03.117. School district data security.** Each school district in the state shall

(1) adopt, implement, and monitor compliance with a data security plan that includes student data security;

(2) implement and monitor compliance with policies and procedures adopted by the board under AS 14.07.165; and

(3) publish and annually update on the district's Internet website, the district's data security plan and explanation of the data fields collected by the district, including the following information:

(A) a description of each student data field;

(B) the reason for the collection of each student data field;

(C) the entities that have access to each student data field;

(D) the location of the server in which the student data field is being stored;

(E) a list of nongovernmental entities that have access to one or more student data fields linked to personally identifiable information;

(F) a description of the safeguards in place for each entity listed under (E) of this paragraph that prevent unauthorized access to personally identifiable information of students.

\* **Sec. 4.** AS 14.03 is amended by adding a new section to article 1 to read:

**Sec. 14.03.200. Definition.** In AS 14.03.015 - 14.03.200, "student data" means

1 (1) electronic information pertaining to an individual student or group  
2 of students collected or reported by a school while the student or group of students  
3 was enrolled in a school in the state or that was accessed or produced by a student or  
4 group of students while enrolled in a school in the state;

5 (2) electronic information pertaining to a student or group of students  
6 that has been or is intended to be transmitted to or stored by a third-party contractor  
7 that provides cloud computing services or other similar services to the school; and

8 (3) electronic mail communications and access information, document  
9 production, and similar electronic information accessed or produced by a student on a  
10 school server.

11 \* **Sec. 5.** AS 14.07.165 is amended to read:

12 **Sec. 14.07.165. Duties.** The board shall adopt

13 (1) statewide goals and require each governing body to adopt written  
14 goals that are consistent with local needs;

15 (2) regulations regarding the application for and award of grants under  
16 AS 14.03.125;

17 (3) regulations implementing provisions of AS 14.11.014(b);

18 (4) regulations requiring approval by the board before a charter school,  
19 state boarding school, or a public school may provide domiciliary services;

20 (5) regulations implementing the secondary school student competency  
21 examination provisions of AS 14.03.075, including the criteria and procedure under  
22 which a governing body uses a waiver to grant a diploma to a student; criteria  
23 regarding granting a waiver must include provisions that a waiver may only be granted  
24 for students who enter the system late or have rare or unusual circumstances meriting  
25 a waiver;

26 **(6) policies and procedures consistent with relevant state and**  
27 **federal privacy laws that**

28 **(A) limit access to individual and redacted student data to**

29 **(i) persons who require access to perform duties**  
30 **assigned by the department, a school district, or the administrator**  
31 **of a public school;**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31

(ii) the student who is the subject of the data and the student's parent, foster parent, or guardian;

(iii) authorized agencies as provided in state or federal law or by an interagency agreement;

(B) restrict student data transfer except as necessary to

(i) comply with federal and state law;

(ii) fulfill student requests;

(iii) carry out a school transfer or student location request; or

(iv) compare multistate assessment data;

(C) prohibit collecting and reporting student data pertaining to

(i) juvenile delinquency records;

(ii) criminal records;

(iii) medical and health records without the written consent of the student's parent or guardian or of a student who is 18 years of age or older or is emancipated under AS 09.55.590;

(iv) biometric information;

(v) political or religious affiliation;

(D) provide for a detailed data security plan for collecting, maintaining, and sharing student data that addresses

(i) privacy;

(ii) authentication;

(iii) breaches in security;

(iv) training;

(v) encryption; and

(vi) other data retention and disposition practices;

(E) except as otherwise provided in AS 14.03.115, prohibit the sharing of student data, including electronic mail addresses and other electronically stored information, for marketing or advertising purposes;

(F) provide for other security measures.

1 \* **Sec. 6.** AS 14.07.165 is amended by adding a new subsection to read:

2 (b) In this section, "student data" has the meaning given in AS 14.03.200.

# ALASKA STATE LEGISLATURE

## REPRESENTATIVE LORA REINBOLD

Session Contact  
State Capitol, Room 432  
Juneau, AK 99801-1182  
Phone - (907) 465- 3822



Interim Contact  
12641 Old Glenn Hwy, Ste. 201  
Eagle River, AK 99577  
Phone - (907) 622- 8950

Official Business

---

### MEMORANDUM

TO: Representative Lynn Gattis, Education Chair

FROM: Representative Lora Reinbold *LOR*

April 7, 2014 \_\_\_\_\_

RE: HB 257 Education Hearing Request

---

At your earliest convenience, I respectfully request a hearing for the HB 257 "An Act relating to restrictions on the collection, storage, and handling of student data" in the House Education Committee.

Please do not hesitate to contact me at (907) 465-3822 with any questions or concerns about this legislation. I look forward to hearing from you and discussing the bill in further detail.

Thank you for your consideration.

28-LS1096P  
Mischel  
4/10/14

**CS FOR HOUSE BILL NO. 257( )**

**IN THE LEGISLATURE OF THE STATE OF ALASKA  
TWENTY-EIGHTH LEGISLATURE - SECOND SESSION**

**BY**

**Offered:  
Referred:**

**Sponsor(s): REPRESENTATIVE REINBOLD**

**A BILL**

**FOR AN ACT ENTITLED**

1 **"An Act relating to restrictions on the collection, storage, and handling of student data."**

2 **BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:**

3 **\* Section 1.** AS 14.03.115 is amended to read:

4           **Sec. 14.03.115. Access to school records [BY PARENT, FOSTER**  
5 **PARENT, OR GUARDIAN].** Upon request of a parent, foster parent, or guardian of  
6 a child under 18 years of age who is currently or was previously enrolled in a  
7 municipal school district or a school district that is a regional educational attendance  
8 area, the school district shall provide a written or electronic copy of the child's  
9 record, including student data, based on the preference of the parent, foster  
10 parent, or guardian. This section does not apply to

- 11                           (1) a record of a child who is an emancipated minor; or
- 12                           (2) record information that consists of the child's address if the school
- 13 district determines that the release of the child's address poses a threat to the health or
- 14 safety of the child.

15 **\* Sec. 2.** AS 14.03.115 is amended by adding a new subsection to read:

1 (b) A school, a district, or the department may use student data that contains  
2 personally identifiable information for a commercial purpose only by first obtaining  
3 written consent, within six months of the use, from the student's parent or legal  
4 guardian or from the student if the student is 18 years of age or older or is emancipated  
5 under AS 09.55.590. Consent must be dated when signed and state the limited purpose  
6 for which the consent is provided and the records that may be used. In this subsection,  
7 "commercial purpose" includes marketing of products or services, compilation of lists  
8 for sale or rent, development of products or services, and the creation of individual,  
9 household, or group profiles.

10 \* **Sec. 3.** AS 14.03 is amended by adding a new section to read:

11 **Sec. 14.03.117. School district data security.** Each school district in the state  
12 shall

13 (1) adopt, implement, and monitor compliance with a data security  
14 plan that includes student data security;

15 (2) implement and monitor compliance with policies and procedures  
16 adopted by the board under AS 14.07.165; and

17 (3) publish and annually update on the district's Internet website, the  
18 district's data security plan, data inventory, and explanation of the data inventory.

19 \* **Sec. 4.** AS 14.03 is amended by adding a new section to article 1 to read:

20 **Sec. 14.03.200. Definition.** In AS 14.03.015 - 14.03.200, "student data" means

21 (1) electronic information pertaining to an individual student or group  
22 of students collected or reported by a school while the student or group of students  
23 was enrolled in a school in the state or that was accessed or produced by a student or  
24 group of students while enrolled in a school in the state;

25 (2) electronic information pertaining to a student or group of students  
26 that has been or is intended to be transmitted to or stored by a third-party contractor  
27 that provides cloud computing services or other similar services to the school; and

28 (3) electronic mail communications and access information, document  
29 production, and similar electronic information accessed or produced by a student on a  
30 school server.

31 \* **Sec. 5.** AS 14.07.165 is amended to read:

1                   **Sec. 14.07.165. Duties.** The board shall adopt

2                   (1) statewide goals and require each governing body to adopt written  
3 goals that are consistent with local needs;

4                   (2) regulations regarding the application for and award of grants under  
5 AS 14.03.125;

6                   (3) regulations implementing provisions of AS 14.11.014(b);

7                   (4) regulations requiring approval by the board before a charter school,  
8 state boarding school, or a public school may provide domiciliary services;

9                   (5) regulations implementing the secondary school student competency  
10 examination provisions of AS 14.03.075, including the criteria and procedure under  
11 which a governing body uses a waiver to grant a diploma to a student; criteria  
12 regarding granting a waiver must include provisions that a waiver may only be granted  
13 for students who enter the system late or have rare or unusual circumstances meriting  
14 a waiver;

15                   **(6) a data inventory that contains individual student data fields for**  
16 **all educational records collected and reported by the department and by school**  
17 **districts and public schools in the state; the board shall annually update and**  
18 **publish on the department's Internet website the data inventory;**

19                   **(7) an explanation of the data inventory adopted under (6) of this**  
20 **subsection; the board shall annually update and publish on the department's**  
21 **Internet website the explanation; the explanation must include, at a minimum,**  
22 **the following information:**

23                               **(A) a description of each student data field;**

24                               **(B) the reason for the collection of each student data field;**

25                               **(C) the entities that have access to each student data field;**

26                               **(D) the location of the server in which the student data field**  
27 **is being stored;**

28                               **(E) a list of nongovernmental entities that have access to**  
29 **one or more student data fields linked to personally identifiable**  
30 **information;**

31                               **(F) a description of the safeguards in place for each entity**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31

listed under (E) of this paragraph that prevent unauthorized access to personally identifiable information of students;

(8) policies and procedures consistent with relevant state and federal privacy laws that

(A) limit access to individual and redacted student data to

(i) persons who require access to perform duties assigned by the department, a school district, or the administrator of a public school;

(ii) the student who is the subject of the data and the student's parent, foster parent, or guardian;

(iii) authorized agencies as provided in state or federal law or by an interagency agreement;

(B) restrict student data transfer except as necessary to

(i) comply with federal and state law;

(ii) fulfill student requests;

(iii) carry out a school transfer or student location request; or

(iv) compare multistate assessment data;

(C) prohibit collecting and reporting student data pertaining to

(i) juvenile delinquency records;

(ii) criminal records;

(iii) medical and health records;

(iv) biometric information;

(v) political or religious affiliation;

(D) provide for a detailed data security plan for collecting, maintaining, and sharing student data that addresses

(i) privacy;

(ii) authentication;

(iii) breaches in security;

(iv) training;

1  
2  
3  
4  
5  
6  
7  
8

(v) encryption; and

(vi) other data retention and disposition practices:

(E) except as otherwise provided in AS 14.03.115, prohibit the sharing of student data, including electronic mail addresses and other electronically stored information, for marketing or advertising purposes;

(F) provide for other security measures.

\* Sec. 6. AS 14.07.165 is amended by adding a new subsection to read:

(b) In this section, "student data" has the meaning given in AS 14.03.200.

# Alaska State Legislature



**Representative Lora Reinbold**  
House District 26

## **Sponsor Summary for House Bill 257**

*"An Act relating to restrictions on the collection, storage, and handling of student data"*

As the educational system merges into the Digital Age it is important that we protect the privacy, security, and confidentiality of student data. Throughout Alaska, and our country as a whole, there has been growing public concern about the collection of personal data. House Bill 257 addresses these concerns and strengthens student digital privacy laws.

HB 257 will enhance data collection transparency to parents and guardians by requiring the State Board of Education to make publicly available an inventory and index of all data elements with definitions of individual student data fields currently in the statewide longitudinal data system. This legislation will also require the establishment of a data security plan, ensuring compliance with federal and state data privacy laws and policies. In addition, HB 257 will prevent the use of student data for commercial purposes without the informed specific consent of a guardian.

I urge your support in this effort to protect Alaska's students from digital privacy gaps.

# Alaska State Legislature



**Representative Lora Reinbold**  
House District 26

## **CS for House Bill 257 – Sectional Analysis**

\* **Section 1:** Amends AS 14.03.115 **Access to School Records.**

Amends the access to school records to include student data based on the preference of the parent, foster parent, or guardian.

\* **Section 2:** Amends AS 14.03.115 by adding a new subsection.

Adds a new subsection which bans the use of student data for “commercial purposes” without the consent of a parent or legal guardian or an 18 year old student.

\* **Section 3:** Amends AS 14.03 by adding a new section 14.03.117.

Adds a new section 14.03.117 “**School District Data Security**”, that requires each school district to adopt, implement, and monitor a data security plan. To increase transparency to parents and guardians the security data plan, a description of each student data field, the reason for collection and additional information will be annually published on a school districts website.

\* **Section 4:** Amends AS 14.03 by adding a new section to article 1 14.03.200 **Definition.**

Adds a section which clearly defines “student data.”

\* **Section 5:** Amends AS 14.07.165 **Duties.**

Amends duties of the board by requiring the adoption of policies and procedures consistent with relevant state and federal privacy laws that limit access to individual and redacted student data.

\* **Section 6:** Amends AS 14.07.165 by adding a new subsection.

Adds a new subsection which refers to AS 14.03.200 for the definition of “student data.”

# Alaska State Legislature



**Representative Lora Reinbold**  
House District 26

## **Proposed CS for House Bill 257 (original version to version "Y")** **Explanation of Changes**

- **Section 1:** Amends AS 14.03.078 **Report**. This section was eliminated.
- **Section 3:** Amends AS 14.03.115 (b) took out "the student or" language that enabled students to give written consent and replaced it to be unless they are 18.
- **Section 4:** Sub section 3 was changed to eliminate the words relating to data inventory and the explanation thereof. Also language from Section 6 subsection 6 and 7 were combined with subsection 3.
- **Section 6:** Subsection 6 and 7 were eliminated and combined under section 4 as previously mentioned. Also subsection 8 (c) was amended to include the release of medical and health records by written consent of a parent or guardian or student 18 years or older.

# Alaska State Legislature



**Representative Lora Reinbold**  
House District 26

## **House Bill 257 - Sectional Analysis**

- \* **Section 1: Amends AS 14.03.078 Report.**  
Updates annual reporting requirements to include a description of changes made to the collection of student data and to include the results of privacy compliance and security audits collected within the previous year.
- \* **Section 2: Amends AS 14.03.115 Access to School Records.**  
Amends the access to school records to include student data based on the preference of the parent, foster parent, or guardian.
- \* **Section 3: Amends AS 14.03.115 by adding a new subsection.**  
Adds a new subsection which bans the use of student data for "commercial purposes" without the consent of a parent or legal guardian.
- \* **Section 4: Amends AS 14.03 by adding a new section 14.03.117.**  
Adds a new section 14.03.117 "School District Data Security", that requires each school district to adopt, implement, and monitor a data security plan. To increase transparency to parents and guardians the security data plan, data inventory, and explanation of the data inventory will be annually published.
- \* **Section 5: Amends AS 14.03 by adding a new section to article 1 14.03.200 Definition.**  
Adds a section which clearly defines "student data."
- \* **Section 6: Amends AS 14.07.165 Duties.**  
Amends duties of the board by requiring the adoption of a data inventory which contains individual student data fields; a detailed explanation of the data inventory; as well as policies and procedures consistent with relevant state and federal privacy laws that limit access to individual and redacted student data.
- \* **Section 7: Amends AS 14.07.165 by adding a new subsection.**  
Adds a new subsection which refers to AS 14.03.200 for the definition of "student data."

# LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES  
LEGISLATIVE AFFAIRS AGENCY  
STATE OF ALASKA

(907) 465-3867 or 465-2450  
FAX (907) 465-2029  
Mail Stop 3101

State Capitol  
Juneau, Alaska 99801-1182  
Deliveries to: 129 6th St., Rm. 329

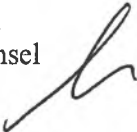
## MEMORANDUM

April 9, 2014

**SUBJECT:** Sectional Summary HB 257; (Work Order No. 28-LS1096\C)

**TO:** Representative Lora Reinbold  
Attn: Elijah Verhagen

**FROM:** Jean M. Mischel  
Legislative Counsel



You have requested a sectional summary of the above-described bill.

As a preliminary matter, note that a sectional summary of a bill should not be considered an authoritative interpretation of the bill and the bill itself is the best statement of its contents. If you would like an interpretation of the bill as it may apply to a particular set of circumstances, please advise.

**Section 1.** Adds to the Department of Education and Early Development's report to the legislature information pertaining to student data and data security audits.

**Section 2.** Requires school districts to provide to a parent or guardian a written or electronic copy of a student record that includes student data.

**Section 3.** Adds restrictions on the use of student data for commercial purposes.

**Section 4.** Requires each school district in the state to adopt, implement, and monitor a plan and policies for student data security and to annually publish the plan, a data inventory, and explanation of the inventory.

**Section 5.** Provides a definition of "student data."

**Section 6.** Adds several duties to the State Board of Education and Early Development that relate to adoption of a data inventory and policies and procedures regarding access to student data.

**Section 7.** Cross-references the definition of "student data" in sec. 5 of the bill for purposes of sec. 6 of the bill.

JMM:ray  
14-168.ray

# Fiscal Note

State of Alaska  
2014 Legislative Session

Bill Version: HB 257  
Fiscal Note Number: \_\_\_\_\_  
( ) Publish Date: \_\_\_\_\_

Identifier: HB257-EED-TLS-04-09-14  
Title: ACCESS TO STUDENT DATA  
Sponsor: REINBOLD  
Requester: House Education Committee

Department: Department of Education and Early Development  
Appropriation: Teaching and Learning Support  
Allocation: Student and School Achievement  
OMB Component Number: 2796

**Expenditures/Revenues**

Note: Amounts do not include inflation unless otherwise noted below. (Thousands of Dollars)

	FY2015 Appropriation Requested	Included in Governor's FY2015 Request	Out-Year Cost Estimates				
			FY 2016	FY 2017	FY 2018	FY 2019	FY 2020
<b>OPERATING EXPENDITURES</b>	<b>FY 2015</b>	<b>FY 2015</b>	<b>FY 2016</b>	<b>FY 2017</b>	<b>FY 2018</b>	<b>FY 2019</b>	<b>FY 2020</b>
Personal Services	309.9		319.3	328.9	338.7	348.9	359.4
Travel							
Services	113.5		78.5	78.5	78.5	78.5	78.5
Commodities							
Capital Outlay							
Grants & Benefits							
Miscellaneous							
<b>Total Operating</b>	<b>423.4</b>	<b>0.0</b>	<b>397.8</b>	<b>407.4</b>	<b>417.2</b>	<b>427.4</b>	<b>437.9</b>

**Fund Source (Operating Only)**

1004 Gen Fund	423.4		397.8	407.4	417.2	427.4	437.9
<b>Total</b>	<b>423.4</b>	<b>0.0</b>	<b>397.8</b>	<b>407.4</b>	<b>417.2</b>	<b>427.4</b>	<b>437.9</b>

**Positions**

Full-time	3.0		3.0	3.0	3.0	3.0	3.0
Part-time							
Temporary							

<b>Change in Revenues</b>							
---------------------------	--	--	--	--	--	--	--

**Estimated SUPPLEMENTAL (FY2014) cost:** 0.0 *(separate supplemental appropriation required)*  
*(discuss reasons and fund source(s) in analysis section)*

**Estimated CAPITAL (FY2015) cost:** 0.0 *(separate capital appropriation required)*  
*(discuss reasons and fund source(s) in analysis section)*

**ASSOCIATED REGULATIONS**

Does the bill direct, or will the bill result in, regulation changes adopted by your agency? Yes  
If yes, by what date are the regulations to be adopted, amended or repealed? 03/31/15

**Why this fiscal note differs from previous version:**

Initial version
-----------------

Prepared By:	Erik McCormick, Director of Assessment, Accountability & Info. Mgmt.	Phone:	(907)465-8686
Division:	Teaching and Learning Support	Date:	04/09/2014 04:46 PM
Approved By:	Mike Hanley	Date:	04/09/14
Agency:	Commissioner		

FISCAL NOTE ANALYSIS

STATE OF ALASKA  
2014 LEGISLATIVE SESSION

BILL NO. HB257

Analysis

Section 1 - 14.03.078 (10), (11) New responsibilities will require additional staff to inventory, review, analyze and report all data collections, forms, elements and reporting requirements that currently exist within EED. This bill will also require EED to make regular updates as new reporting requirements occur or existing requirements change. Under this legislation privacy compliance and security audits will need to be coordinated, conducted and reported for all student data collected. A Project Coordinator position will be needed in order to have independent authority over all student data collected at EED. A Program Coordinator II position will be required to review all forms, update data inventory, provide technical assistance to districts and oversee data collection activities which include the privacy compliance and security audits. An Education Program Assistant position will be needed to support the Project Coordinator and Program Coordinator II as well as provide technical assistance to school districts and individual school staff. These new positions will also be responsible for producing the documentation required under this section.

Project Coordinator	\$131.1
Program Coordinator II	\$110.0
<u>Education Program Assistant</u>	<u>\$ 68.8</u>
Total	\$309.9

Included in the projection is department chargebacks at \$9.5 per employee.

Section 2 - 14.03.115 No anticipated fiscal cost to EED.

Section 3 - 14.03.115 (b) This section addresses utilization of data for commercial purposes. The department does not utilize student data for commercial purpose as defined in this section, therefore no anticipated costs to EED.

Section 4 - 14.03.117 No anticipated fiscal cost to EED.

Section 5 - 14.03.200 New definitions require all documents, reporting forms, data policies, data handbooks be revised. Cost to EED - \$10.0 in the first year only.

Section 6 - 14.07.165 (6) (7) and (8) This bill requires an update to the department's existing data dictionary, a report of all educational records collected and reported by the department and school districts, and documentation or all policies and procedures related to student data. Cost to EED - \$75.0 in the first year, and \$50.0 as continued costs.

Section 7 - 14.07.165 No anticipated fiscal cost to EED.

# LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES  
LEGISLATIVE AFFAIRS AGENCY  
STATE OF ALASKA

(907) 485-3867 or 485-2450  
FAX (907) 485-2029  
Mail Stop 3101


State Capitol  
Juneau, Alaska 99801-1182  
Deliveries to: 129 6th St., Rm. 329

## MEMORANDUM

November 25, 2013

**SUBJECT:** Student privacy rights (Work Order No. 28-LS1096\A)

**TO:** Representative Lora Reinbold  
Attn: Christa Von Bergen

**FROM:** Jean M. Mischel  
Legislative Counsel 

I have received your request for legislation pertaining to student privacy using model legislation prepared by the American Legislative Exchange Council (ALEC). The proposal anticipates the creation of a "data inventory", publication of policies and procedures "to comply with all relevant state and federal privacy laws", record transfer restrictions, "routine and ongoing compliance" with federal and other privacy laws and contracts that govern databases and the like, the establishment of a "chief policy officer" to "assume primary responsibility for privacy policy" hired by each local superintendent, among other things. Although I have drafted some aspects of your request, the legislature may not delegate executive branch policy making functions to specific employees outside of the Administrative Procedures Act (AS 44.62). Please review current state law and let me know how you would like to proceed to avoid redundancies by identifying policy and compliance problems with our current law.

AS 14.03.120(d)(8) already requires compliance with the federal family educational privacy rights law. A copy of the relevant federal statute is enclosed for your review. School districts also use a 10 digit student identifier under 4 AAC 07.060 to provide accountability reports required by the state legislature on school and student performance. If a district fails to comply with state and federal law, the district runs the risk of losing state and federal funding.

In addition, AS 14.03.115 provides that:

Upon request of a parent, foster parent, or guardian of a child under 18 years of age who is currently or was previously enrolled in a municipal school district or a school district that is a regional educational attendance area, the school district shall provide a copy of the child's record. This section does not apply to

- (1) a record of a child who is an emancipated minor; or
- (2) record information that consists of the child's address if the school district determines that the release of the child's

Representative Lora Reinbold  
November 25, 2013  
Page 2

address poses a threat to the health or safety of the child.

I encourage you to check with the department about the specific databases and any compliance issues so that your request can target gaps, if any, in current state law.

If I may be of further assistance, please advise.

JMM:lem  
13-035.lem

Enclosure

Quinn Kendall J.D.  
Director of Government Relations  
Mobil: 314-288-9300  
Email: [Quinn@digitallearningalliance.org](mailto:Quinn@digitallearningalliance.org)  
1725 I Street, NW, Suite 300. Washington D.C. 20006



January 24, 2014

Dear Members of the Alaska Legislature:

On behalf of the Digital Learning Alliance, we write in support of the HB 257: Access to Student Data and urge members of the committee to support the legislation.

Digital Learning Alliance is a national non-profit organization that works to improve economic growth across America by advocating for personalized education through the use of digital learning technologies. We accomplish this mission as we empower legislators and education players with technology solutions in pre-K-12, higher education, and adult learning, resulting in the skilled workforce of the future.

Information infringement is a growing problem in our schools and nation and new steps are needed to ensure we are protected. HB 257 combats such infringements to our children's information and can insure participants that legislatures are doing all they can to protect student's privacy. As a result, we commend Representative Reinbold and HB 257 for taking the necessary precautions to ensure the security of every Alaskan student.

The Alaska Legislature should approve this legislation and likewise, continue to develop proactive measures to pave the way for the implementation of quality digital education solutions. The Digital Learning Alliance stands ready to work with you to develop a proposal that best protects Alaska's students.

All our best,

Quinn Kendall,  
Director of Government Relations; J.D.

[Advanced Search](#)[Funding](#) [Policy](#) [Research](#) [News](#) [About ED](#)**ARCHIVED INFORMATION****Technology in Education: Privacy and Progress****Remarks of U.S. Secretary of Education Arne Duncan at the Common Sense Media Privacy Zone Conference**

FEBRUARY 24, 2014

**Contact:** (202) 401-1576, [press@ed.gov](mailto:press@ed.gov) (<mailto:press@ed.gov>)

I want to thank Jim Steyer and Common Sense Media for bringing this event together and starting this important dialogue – and for your tireless efforts to keep the digital world that our kids inhabit safe and healthy.

America's families, including my own, owe a debt of gratitude to a lot of people here today. Anyone who has children, or works with them, knows that keeping children safe and secure is the most important thing in the world. Privacy is a part of our children's safety and security – especially in our fast-changing world.

Technology has brought the ability to do things that would've seemed like science fiction not long ago.

Our two kids get to hold conversations in full-color video with their grandparents in Australia on a quarter-inch-thick screen that they can hold in their hands – in my childhood that would've seemed like something that Q invented for James Bond.

But technological advances have also brought a host of new worries to parenting. My wife and I constantly feel the need to get smarter about those issues – and so many of the folks in this room are helping America's parents do just that.

I'm also glad to know you will be hearing shortly from Senator Ed Markey, whose work in this area has been so important. And I know that my partner Jim Shelton is going to have a great conversation with Commissioner Julie Brill of the FTC, who is fighting for consumer privacy.

That effort could not be more important now.

A generation ago, a phone was a thing with a wire plugged into the wall, a file went in a drawer, a tablet was something you took if you had a headache, a text was a book that students carried in heavy backpacks, and social media meant watching some TV with your friends.

The new normal embraces a stunning variety of tools and connectedness. In schools, like everywhere else, these new tools and connections have offered extraordinary learning opportunities.

Schools now have not just new ways of working, but vast amounts of new information that can empower teachers, students, and families.

But technological advances have brought with them new cautions. Online banking and email have improved our lives – but they have also given us more to defend. Our identity and privacy are treasures that we must protect in ways we wouldn't have conceived of not too long ago.

People – especially young people – are creating vastly more information than ever before – everything from pictures to news articles to restaurant recommendations and much more.

We can do our banking from a coffee shop or a ski slope! Yet we've never been more worried about inappropriate access to, or use of, our personal information.

This is something we think about a lot at home, with our 12-year old daughter and 10-year old son. Ours is not a low-tech home, although my kids, correctly, claim they have a pretty low-tech dad since they have to share my iPad, and because my wife and I limit their non-educational screen time. We've been learning to code together, though they are ahead of me.

Our kids can access their school assignments on the web, and turn them in, using document sharing. They track their own grades and progress. And we use some web-based tools to support their learning, including online video lessons and foreign language courses.

Of course, all that just scratches the surface of what's possible. We're far from the most advanced house in America.

In education, it would be easy to see the benefits, and the cautions, of this new world as a zero-sum game. I'm going to ask you not to look at it that way.

What I want to say to you today is that the benefits for students of technological advancement can't be a trade-off with the security and privacy of our children.

We must provide our schools, teachers and students cutting-edge learning tools. And we must protect our children's privacy. We can and must accomplish both goals – but we will have to get smarter to do it.

Let's start with why technology matters.

In schools, technology – when it's used wisely – can enable teachers to focus their time on the things they do best, like teaching critical thinking and helping kids who are struggling.

It can provide them up-to-the-minute information on where students are doing well and where they need more help. And it can help them reinvent the most traditional school experiences.

Take what's happening at the Brenda Scott School in Detroit. In one classroom I visited, a teacher named Kristie Ford was working directly with just a few students who immediately needed her help.

The rest were engaged in small-group projects, building 3-D models or working on laptops – a flexibility made possible by digital technology and independent learning plans.

In New York, some schools use a similar strategy to let kids work at their own pace on the material that's right for them – while teachers focus on those who are struggling. Each day, teachers receive a report on each student's progress, and recommendations for learning the next day.

At Nashville Prep, school leaders and teachers analyze data about student achievement, attendance, and discipline every week—as a team—to spot trends and sync up about each student's needs.

And in Huntsville, Alabama, teachers and school leaders can get real-time snapshots of student progress in math. That helps educators to help kids.

The direct benefits to students can be big, too. Just imagine the inspiration that two high school girls, in Kentucky and Virginia, felt when they used open government data to discover a super-fast spinning millisecond pulsar star.

Technology also can empower parents, giving them a stronger connection to what their kids are learning.

Look at Khan Academy, which lets parents look at their children's progress in the language the parent speaks – regardless of the language in which their children are working.

Look at the programs used in Newark and here in DC that generate notes for parents about their children's progress in reading or math—as well as advice about what parents can do to further their kids' learning at home each night.

Now, parents don't have to just ask "what did you do in school" (and, if they're teenagers, have them say, "Nothing"). Now they can start a dialogue about what their kids actually were learning that day!

Here's what these examples – and thousands and thousands more like them – are starting to add up to.

It's about helping teachers work smarter, and helping students learn more quickly and stay more engaged.

It's about helping school systems support teachers more effectively, and helping families stay informed about their kids' education. And it's about parents partnering more actively with children's teachers.

All of that can be transformational. But we must increase access and take on the digital divide with a greater sense of urgency. Some of our international competitors are well ahead of us in providing broadband to their schools – an unacceptable opportunity deficit in our system that President Obama has laid out a plan to fix.

But that's just the beginning. We're behind our international competitors in so many important ways.

Technology can help us catch up – it can help us increase both equity and excellence – if everyone works together to produce solutions that serve students well.

Smart policies will support – not impede – educators who want to put technology to work for kids.

We live in a new, fast-changing time. And in fact, many teachers aren't waiting.

Every day, teachers face the challenge of making education work for each individual child in their classroom, and finding ways to tailor learning to each child's gifts, skills and needs. We need to give teachers every possible tool to help them succeed – but frankly we haven't.

According to a PBS survey, 91 percent of teachers have access to computers—but only one fifth say they have access to the right level of technology.

So no one should be surprised when hard-working, committed teachers go out on their own to find the best tools they can for their classrooms. Whether it's an online grade book, or text message homework reminders, teachers are often finding their own solutions.

Schools and districts need to develop policies that allow rapid adoption of technologies that meet privacy and security standards – and rejection of those that do not.

The practices of districts and schools are changing rapidly as well. Like many organizations, school districts are striving to get smarter about using data to drive improvement.

School systems that have been especially thoughtful in their use of data – like those in Tennessee and Washington, DC – have reaped real learning benefits for kids. And, increasingly, school systems are looking for outside, expert help in analyzing their data.

Like most other organizations these days, district and state educational systems are managing much more digital data. Partly, that's because new technologies are producing more data, and partly because traditional data like bus routes, attendance, food service and business records have moved online.

Like other organizations, school systems often opt to store those data "in the cloud" – meaning, in remote data centers.

To be clear, the motivation here is entirely positive: To find better ways to engage students, to give teachers new tools, to improve instruction, and to help strapped school systems operate more efficiently.

The consequence of all these changes, however, is an exponential growth in the variety and quantity of data. As the use of technology and the quantity of digital data have grown, so have the concerns of parents, and of advocates, like many of you here today.

The questions you are asking are vitally important: What steps are being taken to keep student data secure, and, just as important, to keep outside businesses and other organizations from making inappropriate use of those data?

No one should make the mistake of thinking that these are unreasonable or unimportant questions. In fact, failing to take privacy questions seriously means failing to understand the modern world.

Most days, you don't have to turn far past the front page of the paper to learn something new and unsettling involving personal data. Unwanted revelations can do real and lasting damage. And obviously, the stakes are that much higher when our children are involved.

So I want to be absolutely clear that school systems owe families the highest standard of security and privacy.

No one makes you sign up for Facebook, but you have to go to school. Our expectations for the protection of children must be paramount.

The truth is, in every generation – perhaps now more like every five to ten years – a new revolution in technology forces us to contend with new questions about how to keep our kids safe.

Privacy rules may well be the seatbelts of this generation. I'd like to see vigorous self-policing by the commercial players. Frankly, it's in their interest to do so— and I'm glad to see the conversation starting here.

But I'm not going to wait for industry or rely on promises. It's on all of us – government leaders, advocates, and educators – to act.

This can't be a choice between privacy and progress. It doesn't mean—it can't mean—rolling back the availability of technology.

We know that's a historical impossibility. The toothpaste isn't going back in the tube, and we shouldn't want it to: we cannot stand between teachers and the tools they need to do their jobs and reach every child where they are.

On the contrary, we need to do a far better job of getting useful technology to educators, students, and families that deepens and accelerates learning.

We cannot ask our schools to choose between privacy and progress. School systems must have the ability to use data to get their basic business done — whether that involves organizing bus routes or analyzing instructional information.

None of that conflicts with a powerful commitment to privacy.

Protecting our students' information is more than a legal requirement – it's a moral imperative. Our children's privacy is not for sale and must not be put at risk.

Personal information that students and families provide for educational purposes should be used for educational purposes only. And both school systems and technology providers should have appropriate policies for how they handle data.

Taking action on those principles involves laws and policies, but it's also a matter of priorities and clear, consistent communication.

On the legal side, as most of you here know, three keystone federal laws protect student privacy: The Family Educational Rights and Privacy Act, The Protection of Pupil Rights Amendment, and the Children's Online Privacy Protection Act.

Together, these statutes place significant limits on how student information can be used.

But these are complex issues, and the field is developing rapidly – which is why we're committed to stepping up the pace at which we provide guidance to help school systems and educators interpret the law, including examples of best practice.

Tomorrow, we will release new guidance, with more coming in the weeks ahead.

Our Administration takes these issues seriously. That's why I appointed the first-ever executive-level Chief Privacy Officer in the Department of Education, Kathleen Styles, who has helped us to start offering technical assistance to

states, districts and schools, around student privacy. Kathleen has been fantastic, and I thank her for her leadership. We established the Privacy Technical Assistance Center to provide that hands-on help.

But federal law provides only some of the guard rails for data and privacy practice. Much of the control over these issues lies in the policies of states and districts.

And, for the record, the Department of Education itself isn't allowed to create a national database of individual student-level information, aside from mandated purposes like college loans. We don't, we haven't, and we won't do that—period.

And nothing about the new assessments, developed by consortia of states as part of new, higher standards, changes that.

But there's a lot of hard work ahead. As an education community, we have to do a far better job of helping teachers and administrators understand technology and data issues. And we need to do a better job reaching the general public too.

Too often, the public discussion on these issues has become muddled, conflating separate issues.

For example, the mere fact that student data is stored in the cloud doesn't mean that it is used for an improper purpose, or that unauthorized parties or vendors have access to it. Data stored in the cloud can actually be more secure than data stored on a computer at a school. But too many families today have been led to believe that remote storage of student data means it's up for sale.

Put plainly, student data must be secure, and treated as precious, no matter where it's stored. It is not a commodity. In truth, while we have seen security breaches in schools — with both paper and digital records — we have seen few significant instances of systemic misuse of student data.

As you know, though, many of our school systems have work to do to bring policy into line with fast-changing technologies. This isn't a matter of bad intention; it's a matter of priorities. And for our schools, privacy needs to be a higher priority.

Schools and school systems should be asking themselves some hard questions. Here are five quick examples:

- Do you know what online services your schools and teachers are using?
- Are you offering teachers timely approval of technology they want to use?
- Do your contracts explicitly lay out the ownership and appropriately limit the use of any data collected?
- Are you transparent with parents about how your district uses data?
- Do your schools allow students to bring their own devices as tools for learning, and do your policies protect them?

Some districts and states are demonstrating real leadership and thoughtfulness in these areas, and we all can learn from them. For example, the Kansas State Department of Education has developed an innovative data quality certification program to train staff on data quality practices and techniques, including privacy and security.

And closer to home, Fairfax County tests software and applications to verify that vendor security and privacy promises are accurate.

But the responsibility here doesn't lay just with schools systems. Technology providers need to shoulder their responsibility for ensuring the privacy of our students as well.

There's plenty of energy, in this room and around the country, for stronger regulation of your work. Let me say this clearly: It is in your interest to police yourselves before others do.

In part, that means being transparent — not with hundred-page user agreements spread across multiple screens, but with language that parents and educators can easily understand.

It means offering districts something better than take-it-or-leave-it "Click Wrap" agreements that allow the provider to unilaterally amend its privacy practices — without even telling the district. That doesn't build long-term confidence and trust. Please demonstrate that you know what it means to be a leader for our kids, and for us, as their parents.

While I am challenging everyone in this room, I want to make clear that we challenge ourselves, every day, at the Department to be part of the solution.

First, we enforce the statutes we administer. There are important legal safeguards against misuse and commercialization of student data, and we will enforce these safeguards.

Second, we will continue to offer guidance and technical assistance to schools and districts around student privacy — as well as guidance and technical assistance around the use of education data and technology.

As the field develops, we are working to stay current and be helpful. Where we fall short, please push us. We need your best ideas—we want to be challenged.

Let me close with the bottom line: Personal data in education should be used only for educational purposes, not to sell students snack foods or video games.

Parents and schools need clear information that enables them to make good choices. In protecting our children, we all have a role to play.

So I want to challenge advocates, tech leaders, software vendors, educators, policymakers – to make protecting our students’ privacy a higher priority.

I want to applaud the hard work and leadership of so many of you here to make that happen.

Together, we can and we must harness the extraordinary potential of technology to empower teachers, students and families – without faltering in our duty to protect them.

**Tags:**

Tweet 64

Like 37

---

**Notice of Language Assistance:** [English](#) | [español](#) | [中文：繁體版](#) | [Việt-nam](#) | [한국어](#) | [Tagalog](#) | [Русский](#)