HOUSE OF REPRESENTATIVES

SB 1306

schools; data privacy

Sponsors: Senators Ward, Yee: Allen, et al.

DPA Committee on Education

X Caucus and COW

House Engrossed

OVERVIEW

SB 1306 makes changes to the Arizona Department of Education's (ADE) education data system privacy and confidentiality requirements.

HISTORY

Laws 2010, Chapter 334, established the Data Governance Commission (Commission) to identify, examine and evaluate the needs of public institutions that provide instruction to K-12 grades and postsecondary students. The Commission establishes guidelines relating to managed data access, technology, privacy and security and provides recommendations on technology spending, access privileges and access management and the control of data confidentiality and data security for stored and transmitted data (Arizona Revised Statutes (A.R.S.) § 15-249.01).

A.R.S. 15-1041 establishes the Student Accountability Information System (SAIS) to enable school districts, joint technical education districts and charter schools to transmit student level data and school finance data electronically to ADE. Statute requires any disclosure of educational records compiled by ADE to comply with the Family Educational Rights and Privacy Act (FERPA), a federal law that protects the privacy of student education records (ed.gov). Additionally, A.R.S. § 15-1045 requires ADE to maintain the database to limit the use of information to comply with statutory obligations, ensure that personally identifiable information is confidential and not public record, employ proper security measure to ensure the confidentiality and integrity of the education database and secure data from breaches and identity theft.

A.R.S. § 15-1042 defines *student level data* as all data elements that are compiled and submitted for each student in the state that are necessary for the completion of the statutory requirements of ADE and the Arizona State Board of Education (SBE) relating to the calculation of funding for public education, the determination of student academic progress as measured by student testing programs in this state, state and federal reporting requirements and other duties prescribed to ADE or SBE by law. *Student level data* does not include data elements related to student behavior, discipline, criminal history, medical history, religious affiliation, personal physical descriptors or family information not authorized by the parent or guardian of the pupil or otherwise required by law.

PROVISIONS

Data Governance Commission

1. Directs the Commission to create, publish and make publicly available on ADE's website a data dictionary with definitions of individual student data elements in the education data system, including the following:

   a. Elements that are required to be reported by state and federal education mandates.
   b. Elements that have been proposed for inclusion in the education data system with a statement regarding the purpose or reason for the proposed collection.
   c. Elements that are collected or maintained without a currently identified purpose.

2. Requires the Commission to review and approve data elements to be included in the education data system.
   a. Requires any new student data collection to be announced to the general public and posted for at least a 60 day review and comment period.

3. Expands the information required in the Commission's annual report to include the following:
   a. New data elements proposed for inclusion in the education data system.
   b. Changes to existing data collections required for any reason, including changes to federal reporting requirements.
   c. An explanation of exceptions granted by ADE regarding the release of student level data out of state.
   d. The results of any privacy or security audit conducted within the previous year, except information that would pose a threat to the security or confidentiality of the education data system or the secure transmission of data between school districts, charter schools and ADE.

Data Confidentiality

4. Directs ADE to develop criteria for the approval of data requests from state and local agencies, the Legislature and researchers.
   a. Directs ADE to release masked student level data unless otherwise allowed by law or if ADE determines the request to qualify for an exception under FERPA.

5. Replaces references to the ADE *education database* with *education data system*.

6. Deletes existing requirements for ADE database maintenance.

7. Reinserts the requirement for personally identifiable information and student level data contained in the education data system to be confidential and not public record.

8. Directs ADE to create a unique pupil identifier for each student in the education data system.

9. Directs ADE to develop, publish and make publically available policies and procedures to comply with all relevant state and federal privacy laws, including FERPA.

10. Instructs ADE's developed policies to require:
    a. Access to student level data in the education data system be limited to:
       i. Authorized ADE staff that require access to perform assigned duties required by law, interagency data sharing agreements or other legal obligations.
       ii. School district and charter school administrators, teachers and personnel who require access to perform assigned duties.
       iii. Students and the parents of the student, except that accessible information is limited to data about that student.
       iv. The authorized staff of other state agencies in the state or political subdivisions as required by law or prescribed by interagency data sharing agreements.
       v. Researchers conducting approved studies.

b. ADE only use aggregated data that does not contain personally identifiable information in public reports and in response to public records requests, except as provided by law.
c. Students and parents be notified of private rights concerning educational records under federal and state law.

11. Prohibits ADE from transferring student level data deemed confidential to any federal agency or state or local agency, unless allowed by law.

12. Requires ADE to develop and implement a detailed security plan that includes the following:
    a. Procedures for authorizing access to the education data system and student level data.
    b. Standards for compliance with federal and state privacy laws and regulations.
    c. Privacy and security audits.
    d. Planning for a possible breach of data security, including notification procedures to entities that own data that may be affected by the data breach.
    e. Data retention and destruction policies consistent with the Arizona State Library, Archives and Public Records (ASLAPR) adopted guidelines.
    f. Compliance with statewide technology security standards adopted by the Arizona Department of Administration, at a minimum.

13. Directs ADE to ensure that any contracts with private vendors governing databases, assessments or instructional supports that contain student level data include express provisions for safeguarding privacy and security and civil penalties for noncompliance.

14. Prohibits school districts and charter schools from reporting the following student level data to ADE:
    a. Juvenile delinquency records.
    b. Criminal records, except incident data required for school safety purposes.
    c. Medical and health records.

15. Prohibits school districts and charter schools from collecting the following data for any student:
    a. Political affiliation.
    b. Religious affiliation.
    c. Biometric information, except as allowed by law.
    d. Firearms ownership.

ADE Chief Privacy Officer and Chief Data Officer

16. Directs the Superintendent of Public Instruction to appoint a chief privacy officer to assume primary responsibility for agency private policy.

17. Enumerates the following duties of the chief privacy officer:
    a. Ensure the use of technology sustains and does not erode privacy protections.
    b. Ensure that student level data contained in the education data system is handled in full compliance with applicable state and federal laws.
    c. Evaluate, in conjunction with the chief data officer, legislative and regulatory proposals involving the collection, use and disclosure of student data by ADE.
    d. Conduct, in conjunction with the chief data officer, a privacy impact assessment on proposed ADE rules and on the privacy of student data, including the type of personal information collected and the number of students affected.

e. Coordinate with the Attorney General and chief data officer to ensure programs, policies and procedures affecting civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.
f. Establish and operate a process for parents to file complaints of possible privacy violations and provide redress procedures.
g. Ensure that all privacy-related incidents are properly reported, investigated and mitigated as appropriate.
h. Work with the chief data officer to provide training, education and outreach to build a culture of privacy throughout ADE.
i. Conduct investigations and submit reports relating to the administration of programs and operations of ADE regarding privacy matters.

18. Grants the chief privacy officer access to all records, reports, audits, reviews, documents, papers, recommendations and other materials available to ADE that are necessary to complete the responsibilities of the office.

19. Directs the chief information officer of ADE to appoint a chief data officer.

20. Enumerates the following duties of the chief data officer:
    a. Coordinate with the chief privacy officer to fulfill the duties of the office.
    b. Establish policies and procedures to ensure the efficient and secure collection, storage, maintenance and disposition of all data collected in the education data system according to applicable laws.
    c. Establish policies necessary for implementing fair information practice principles to enhance privacy protections.
    d. Work with the chief privacy officer and other officials in engaging stakeholders about the quality, usefulness, openness and privacy of data.
    e. Establish and operate, in coordination with the chief information officer, a privacy incident response program.

Miscellaneous

21. Authorizes ADE to assess fees for requests for the production of data or for the assembly of data that is otherwise confidential and not public record into aggregated reports that are not already available.

22. Allows a student's parent or legal guardian to request to review a copy of the student's educational record, including data submitted to the education data system, using statutory processes.

23. Eliminates the requirement for ADE to grant a school district, Joint Technical Education District or charter school an extension to student level data submission deadlines and the authority for ADE to allow for an alternative method of submission if the school or district shows good cause and the school or district will continue receiving monies for educating students.

24. Requires student immunization records to be maintained according to ASLAPR standards rather than as part of a mandatory permanent student record.

25. Repeals the Arizona E-Learning Task Force.

26. Defines terms for all statutes pertaining to SAIS.

27. Makes technical and conforming changes.

AMENDMENTS

Committee on Education

1. Requires a school service provider (provider) to:
   a. Provide clear materials about the types of student personal information (information) the provider collects and how that information will be used and shared.
   b. Provide prominent notice before making material changes to privacy policies.
   c. Facilitate access to and correction of information by students and parents or guardians.
   d. Obtain consent prior to using information in a manner inconsistent with the provider's privacy policy.
      i. Requires a provider to obtain consent from a student's parent or guardian or the student if information is collected directly from students.
      ii. Permits the school district, charter school or teacher to provide consent in all other cases.
   e. Maintain a comprehensive security program.
   f. Require any third party involved on the provider's behalf to adhere to the same requirements as the provider.
   g. Delete information within a reasonable period of time if the school district, charter school or teacher requests the deletion of data, unless the provider has obtained consent to retain the information by the student or his/her parent or guardian or the student has transferred to another school district, charter school or teacher who has requested the information be retained.

2. Allows a provider to offer to a public school or teacher changes to privacy policies and the types and use of information by a school service provider.

3. Permits a provider to collect, use and share information only for the purposes authorized by the school district, charter school, teacher, parent, guardian or student.
   a. Specifies that this prohibition does not apply to the purchase, merger or other type of acquisition of a provider or a provider's assets by another entity, provided the successor entity continues to be subject to this Act.

4. Prohibits a provider from:
   a. Selling information.
   b. Using or sharing information to target advertisements towards students.
   c. Using information to create a personal profile for any other purpose than those permitted by the school district, charter school, teacher, parent, guardian or student.
      i. Stipulates that *create a personal profile* does not include the collection and retention of account records or information that remains under the control of the student, parent, school or school district.

5. Exempts providers from the requirements of this Act for existing contracts, until the next renewal date of the contract.

6. Stipulates that the following is not prohibited:
   a. Using information for adaptive learning, personalized learning or customized education.
   b. Using information for maintaining, developing or diagnosing the school service's site, service or application.
   c. Providing recommendations for school, educational or employment purposes within a school service's site, service or application without the response being determined by payment or other consideration from a third party.

d. Responding to a student's request for feedback without the response being determined by payment or other consideration from a third party.
e. Disclosing information to:
   i. Ensure legal or regulatory compliance or protect against liability.
   ii. Protect the security or integrity of its site, service or application.
   iii. Respond to or participate in judicial process.
   iv. Protect the safety of users or security of the school service's site, service or application.
   v. To a service provider provided the school district contractually prohibits the use of information for any other purpose than providing the contracted service, prohibits the service provider from disclosing any information to a third party unless expressly permitted and requires the service provider to comply with this Act.

7. Prohibits this Act from being construed to impede the ability of students to download, export or otherwise save or maintain their own student data.

8. Provides that this act may be cited as the "Student User Privacy in Education Rights Act" or the "SUPER Act."

9. Defines terms.