



**ARIZONA STATE SENATE**  
*Fifty-Second Legislature, First Regular Session*

FACT SHEET FOR S.B. 1306

schools; data privacy

Purpose

Modifies various statutes governing student data privacy and the Department of Education's (ADE) student information database.

Background

***Student Accountability Information System (SAIS)***

The SAIS was established to enable school districts, joint technical education districts (JTEDs) and charter schools to transmit student level data and school finance data electronically to ADE for the purpose of complying with the statutory obligations of ADE and the State Board of Education (SBE) (A.R.S § 15-1041). ADE must notify school districts, JTEDs and charter schools of electronic data submission procedures and must distribute a list of the specific student level data elements, including the statutory or regulatory reference for each data element, that school districts, JTEDs and charter schools are required to submit. ADE must grant a school district, JTED or charter school an extension to the deadline for the submission of student level data or may provide for an alternative method for the submission of student level data if the school district, JTED or charter school proves that good cause exists for the extension. The request for an extension of the deadline for the submission of student level data must include a justification for the extension and the status of current efforts towards complying with the submission of student level data (A.R.S § 15-1042).

***Education Learning and Accountability System (AELAS)***

ADE implements the AELAS to collect, compile, maintain and report student level data for students attending public educational institutions that provide instruction to pupils in preschool programs, kindergarten programs, grades one through twelve and postsecondary educational programs in this state (A.R.S § 15-249).

***Family Educational Rights and Privacy Act (FERPA)***

FERPA is a federal law enacted in 1974 that allows a parent certain rights with respect to their child's education records. These rights transfer to the student when he or she reaches 18 years of age or attends a school beyond the high school level. Students to whom the rights have transferred are known as *eligible students*. Parents or eligible students have the right to inspect and review the student's education records maintained by the school and the right to request that a school correct records that the parent or eligible student believes to be inaccurate or misleading. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows

schools to disclose those records, without consent, to the following parties or under the following conditions: 1) school officials with legitimate educational interest; 2) other schools to which a student is transferring; 3) specified officials for audit or evaluation purposes; 4) appropriate parties in connection with financial aid to a student; 5) organizations conducting certain studies for or on behalf of the school; 6) accrediting organizations; 7) to comply with a judicial order or lawfully issued subpoena; 8) appropriate officials in cases of health and safety emergencies; and 9) state and local authorities, within a juvenile justice system (34 Code of Federal Regulations § 99.31).

### ***Children's Online Privacy Protection Act (COPPA)***

According to the Federal Trade Commission's website, COPPA is a federal law enacted in 1998 that applies to the online collection of personal information from children under age 13. COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. The rules spell out what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online.

### ***Data Governance Commission (DGC)***

The DGC is established in ADE and consists of 14 members. The DGC is required to identify, examine and evaluate the needs of public institutions that provide instruction to pupils in preschool programs, kindergarten programs, grades one through twelve and postsecondary programs in Arizona. The DGC's guidelines must address: 1) managed data access; 2) technology; 3) privacy and security; 4) adequacy of training; 5) adequacy of data model implementation; 6) prioritization of funding opportunities; 7) resolution of data conflicts; and 8) the form and format of data elements that are required for state and federal reporting and interagency data sharing. They also provide recommendations on technology spending, provide certain analyses and recommendations and ensure that the guidelines and recommendations adopted reduce duplication and administrative requirements for public schools, postsecondary institutions and public agencies (A.R.S. § 15-249.01).

### ***E-learning Task Force***

The E-learning Task Force is required to: 1) examine e-learning programs in other states; 2) analyze potential methods to implement e-learning programs in Arizona; 3) develop innovative e-learning solutions; 4) submit specified recommendations to the Legislature and the SBE; 4) collaborate with the Department of Administration and other public and private entities to express the technology needs of schools in this state; and 5) annually report to the Legislature regarding e-learning programs and solutions (A.R.S § 15-1044).

There is no anticipated fiscal impact to the state General Fund associated with this legislation.

Provisions

*Education Data System (EDS)*

1. Revises previous statutes governing ADE's education database of pupil records by establishing the EDS.
2. Defines the *Education Data System* as the SAIS, or its successor system, and the AELAS, or its successor system, and the respective components of the SAIS and AELAS.
3. Specifies that personally identifiable information and student level data contained in the EDS is confidential and is not a public record.
4. Directs ADE to create a unique pupil identifier for each pupil in the EDS.
5. Requires ADE to develop, publish and make publicly available policies and procedures to comply with all relevant state and federal privacy laws, including FERPA.
6. Mandates EDS policies to require that access to student level data in the EDS be restricted to:
  - a) authorized ADE staff who require access to perform assigned duties as required by law, by interagency data sharing agreements or other legal obligations;
  - b) school district and charter school administrators, teachers and personnel who require access to perform assigned duties;
  - c) students and parents or legal guardians of students, except access be limited to data about that particular student; and
  - d) authorized staff of other state agencies in Arizona or political subdivisions of Arizona as required by law or as prescribed by interagency data sharing agreements.
7. Requires EDS policies to require:
  - a) ADE to use only aggregated data that does not contain personally identifiable information in public reports and in response to public records requests, unless authorized by a statutory exemption; and
  - b) students and parents be notified of privacy rights concerning educational records under federal and state law.
8. Prohibits ADE from transferring student level data deemed confidential by statute to any federal agency or any state or local agency, unless otherwise permitted by law.
9. Requires ADE to develop and implement a detailed security plan that includes:
  - a) procedures for authorizing access to the EDS and to 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;
  - e) data retention and destruction policies consistent with guidelines adopted by the Arizona Library, Archives and Public Records; and
  - f) at a minimum, compliance with statewide technology security standards adopted by the Department of Administration.

10. Mandates ADE ensure any contracts with private vendors governing databases, assessments or instructional supports that include student level data include express provisions that safeguard privacy and security and include penalties for noncompliance.
11. Prohibits school districts and charter schools from reporting to ADE the following student level data:
  - a) juvenile delinquency records;
  - b) criminal records, except incident data required to be reported for school safety purposes; and
  - c) medical and health records.
12. Forbids school districts and charter schools from collecting any of the following pupil data:
  - a) political affiliation;
  - b) religious affiliation;
  - c) biometric information, unless permitted through written permission from the pupil's parent or guardian; and
  - d) firearm ownership.

*ADE Chief Privacy Officer & Chief Information Officer*

13. Requires the SPI to appoint a Chief Privacy Officer who must assume primary responsibility for the agency privacy policy.
14. Grants the Chief Privacy Officer access to the following:
  - a) records;
  - b) reports;
  - c) audits;
  - d) reviews;
  - e) documents;
  - f) papers;
  - g) recommendations; and
  - h) other materials available to ADE that are necessary to complete the Chief Privacy Officer's responsibilities.
15. Directs the Chief Privacy Officer to:
  - a) ensure the use of technologies sustain, and do not erode, privacy protections;
  - b) ensure student level data contained in the EDS is handled in full compliance with state and federal laws;
  - c) coordinate with the Attorney General and Chief Data Officer to ensure programs, policies and procedures affecting civil rights and liberties and privacy considerations are addressed in an integrated and comprehensive manner;
  - d) establish and operate a process for parents to file complaints of possible privacy violations, including FERPA violation complaints, and to provide redress procedures;
  - e) ensure all privacy-related incidents are properly reported, investigated and mitigated as appropriate;
  - f) work with the Chief Data Officer to provide training, education and outreach to build a culture of privacy throughout ADE; and

- g) make investigations and submit reports regarding the administration of programs and operations of ADE regarding privacy matters.

16. Directs the Chief Information Officer of ADE to appoint a Chief Data Officer and charges the Chief Data Officer to:

- a) coordinate with the Chief Privacy Officer to fulfill statutory EDS requirements;
- b) establish policies and procedures to ensure the efficient and secure collection, storage, maintenance and disposition of all data collected in the EDS according to applicable laws;
- c) establish ADE 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; and
- e) establish and operate an ADE privacy incident response process in coordination with the Chief Information Officer.

17. Requires the Chief Privacy Officer, in conjunction with the Chief Data Officer, to:

- a) evaluate legislative and regulatory proposals involving collection, use and disclosure of student data by ADE; and
- b) conduct a privacy impact assessment on proposed rules of ADE in general, and the proposed rules of ADE on the privacy of student data, including the type of personal information collected and the number of students affected.

***Data Governance Commission (DGC)***

18. Requires the DGC to create, publish and make publicly available on ADE's website a data dictionary with definitions of student data elements in the EDS, including any student data element:

- a) that is required to be reported by state and federal education law;
- b) that has been proposed for inclusion in the EDS with a statement regarding the purpose or reason for the proposed collection; and
- c) that ADE collects or maintains without a currently identified purpose.

19. Requires the DGC to review and approve data elements to be included in the EDS.

20. Requires any proposed new student data collection to be announced to the general public and posted for a review and comment period of at least 60 days.

21. Requires the DGC to include in the DGC's annual report:

- a) any new data elements proposed for inclusion in the EDS;
- b) changes to existing data collections required for any reason, including changes to federal reporting requirements;
- c) an explanation of any exceptions granted by ADE during the year regarding the release of student level to any federal agency or another state or local agency; and
- d) the results of any privacy or security audit conducted within the previous year.

22. Prohibits the DGC's annual report from including any information that would pose a threat to the:

- a) security or the confidentiality of the EDS; or
- b) secure transmission of data between school districts, charter schools and ADE.

***Third-Party Provider Contracts***

23. Allows local educational agencies to enter into a contract with a third-party provider for either or both of the following purposes:

- a) to provide services, including cloud-based services, for the digital storage, management and retrieval of pupil records; and
- b) to provide digital educational software that authorizes a third-party provider to access and acquire pupil records.

24. Requires the contract to contain the following:

- a) a statement that pupil records continue to be the property of and under the control of the local educational agency;
- b) a description of the procedures by which a parent, guardian or eligible pupil may review the pupil's records and correct erroneous information;
- c) a description of the third-party provider's actions including the designation and training of responsible individuals to ensure security of pupil records;
- d) a description of the procedures for notifying the affected parent and pupil if an unauthorized disclosure of the pupil's records occurs;
- e) a certification, upon completion of the terms of the contract, that pupil records will not be retained or available to the third-party provider including a description of how the certification will be enforced; and
- f) a description of how the local education agency and the third-party provider will jointly ensure compliance with state and federal laws including FERPA and COPPA.

25. Requires the contract to prohibit third-party providers from using:

- a) personally identifiable information in pupil records for commercial or advertising purposes; and
- b) any information in the pupil record for any purpose other than for the requirements of the contract.

26. Stipulates that compliance with the contract's description of the third-party provider's actions and training to ensure the security of pupil records does not absolve the third-party provider of liability in the event of an unauthorized disclosure of pupil records.

27. Specifies that a contract that fails to comply with the requirements is voidable and requires all pupil records in the possession of the third-party provider to be returned to the local education agency.

28. Excludes contracts that were executed before October 1, 2015 from the requirements of this section until the expiration, amendment or renewal of those contracts.

*Miscellaneous*

29. Requires ADE to develop criteria for the approval of data requests from state and local agencies, the Legislature and researchers if ADE determines the request qualifies for an exception under FERPA.
30. Requires student level data to remain redacted at all times unless the sharing of student level data is specifically permitted by law.
31. Authorizes ADE to assess fees for complying with requests for the following:
  - a) production of data for qualifying data requests from state and local agencies, the Legislature and researchers; or
  - b) assembly of data that is otherwise confidential and is not a public record into aggregated reports not already available from ADE.
32. Allows a student's parent or legal guardian to request to review a copy of the student's education record, including data submitted to the EDS, in accordance with a statutory request process.
33. Requires the school immunization record to be maintained according to standards set by the Arizona State Library, Archives and Public Records.
34. Repeals the Arizona E-Learning Task Force.
35. Eliminates the ability for ADE to grant an extension to the deadline for the submission of student level data or provide for an alternative method for the submission of student level data if a good cause exists for the extension to:
  - a) school districts;
  - b) JTEDs; or
  - c) charter schools.
36. Includes the existing definition of *student level data* in the SAIS section of statute and defines the following:
  - a) *aggregated data*;
  - b) *local education agency*;
  - c) *personally identifiable information*;
  - d) *public records*;
  - e) *third-party provider*; and
  - f) *unique pupil identifier*.
37. Makes technical and conforming changes.
38. Becomes effective on the general effective date.