NASSP™ National Association of Secondary School Principals

POLICY ISSUE BRIEF:
STUDENT DATA PRIVACY

Issue at a Glance

Data-driven decision-making has become a tenet of high-performing schools and is essential to transforming teaching and learning. Data and learning analytics can personalize learning for many more students and increase student retention and achievement in the highest-need schools. Technology has made it easier for principals and teachers to collect and analyze data at the school level, and districts and states are now creating longitudinal database systems to help them make structural changes in education that will have a greater impact on more students.

For this reason, educators at all levels are authorizing third-party vendors to have access to student data. These vendors offer services that educators believe will assist them in communicating with parents, improving the quality of education programs, providing supports and services for students, and providing secure data storage. In fact, every electronic device and application with a connection to the internet could potentially be used to collect or access student data.

While the collection and analysis of student data is essential to teaching and learning , it must be done within strict parameters that protect the privacy of students and ensure that their data is used only for legitimate educational purposes. The Family Educational Rights and Privacy Act (FERPA) was enacted in 1974 and generally prohibits schools from disclosing personally identifiable information in students' education records without consent. There are exceptions to the consent requirement, including one that allows the disclosure of such information to "school officials" for educational purposes.

This particular provision was expanded in 2008 when the U.S. Department of Education approved new regulations clarifying that third-party vendors (such as those helping manage school databases or provide digital curriculum) can be included within the "school officials" exception. In addition, the Protection of Pupil Rights Amendment requires school districts to notify parents if personally identifiable information will be used for marketing purposes; and the Children's Online Privacy Protection Act requires parental consent before collecting, using, or disclosing personal information from children under the age of 13. While third parties must be under the direct control of the school in terms of how they use and maintain the records and only use the records for the purposes for which they were shared, there is some concern that there are still gaps in the protection of student data.

While most policymakers and educators understand the value of data collection in improving educational quality, there is some concern that FERPA itself, as well as the accompanying regulations, has become outdated in the new digital age. Hundreds of bills have been proposed in Congress in recent years to update FERPA. Meanwhile, almost every state has passed some new policy in the past 10 years to update their own student data privacy standards and protection measures with over 150 new laws enacted across the country as of 2026. Each principal's full understanding of and familiarity with federal, state, and district policies on data collection and student privacy requirements are essential as this issue further develops.

NASSP Position

- NASSP believes that data has the power to transform teaching and learning by helping educators identify and provide supports to all students, assisting teachers and school leaders in improving their instructional practices, and informing schoolwide improvement activities.
- NASSP believes that student data should only be used for the purpose of informing education policy, practice, and research, and to deliver educational services to students.
- NASSP believes that technology-enhanced data collection and analysis can assist schools in the planning and delivery of a student-centered, personalized, and individualized learning experience for each student.
- Federal laws to update FERPA and student data privacy must allow states to maintain the integrity of the laws they have already passed and allow school districts to effectively use student data for educational purposes.
- NASSP has separate policy issue briefs on Digital Equity, Artificial Intelligence, and School Safety that provide additional recommendations and resources.

Recommendations for Federal Policymakers

- Review policies on the use of student data to ensure they balance privacy protection with the need to improve teaching and learning.
- Require all entities that collect and/or store sensitive student data to maintain a comprehensive security program that is designed to protect the security, privacy, confidentiality, and integrity of personally identifiable information against risks.
- Provide guidance to states regarding the collection, storage, security protections, and destruction of student data.
- Provide funding to states and districts to help them address privacy issues related to student data, including training and professional development for educators, technology capacity, and technical support
- Ensure that personal information and online learning activities are not used to target non-education related advertising to students or their families.
- Limit nonconsensual access to personally identifiable student data to school, district, or state educational agency employees and to authorized service providers under their direct control and solely for the authorized educational purpose.
- When considering updates to FERPA or other laws governing student data collection in proposed legislation such as the Kids Online Safety Act, ensure that there is not broad preemptive language that would invalidate state laws regulating education technology vendors who receive student data when providing services for schools.
- Recognize that many schools use collaborative learning and/or gamified education technology platforms to enhance learning, and if laws are passed to regulate the industry, exceptions must be made to ensure that learning via these technologies is not disrupted. Examples of recent legislation include:
  - The Algorithmic Choice and Transparency Act requires online platforms to give users an option to easily switch between personalized recommendation systems and input-transparent algorithms. As written, the bill could allow students to unilaterally decide to circumvent using an adaptive learning product that their school has carefully vetted for privacy and security safeguards and contracted to use to improve learning.

- The Safer Guarding of Adolescents from Malicious Interactions on Network Games (GAMING) Act requires online video game providers to limit minors' ability to communicate with other users by default and says that parents are the only ones who can disable the safeguards. This may unintentionally restrict students' ability to communicate with teachers and their classmates on gamified edtech platforms used in class.

Recommendations for State Policymakers

- Establish a statewide data security plan to address administrative, physical, and technical safeguards for state data systems and other state data collection.
- Develop data breach notification policies for districts and schools.
- Identify a state-level official who is responsible for privacy, data security, and compliance with all federal and state privacy laws and regulations.
- Develop policies on data collection, storage, and access to ensure that student data collected through statewide longitudinal data systems is protected from inappropriate sharing or use.
- Provide guidance to districts and schools regarding the collection, storage, security protections, and destruction of student data.

Recommendations for Districts Policymakers

- Develop clear policies about what student information is collected, how that data is used, to whom the data is disclosed, and each party's responsibilities in the event of a data breach.
- Ensure that data security practices include proper data deletion and disposal, including the purging of electronic data, shredding physical documents, and destroying the presence of all data on old electronic equipment where data has been stored.
- Identify a district privacy officer who is responsible for monitoring and complying with federal, state, and district policies on data privacy and for guiding school leaders and teachers in their use and protection of data.
- Provide training for all district staff to ensure they understand basic legal requirements, their responsibilities, and specific district policies concerning student data.
- Ensure that principals receive training on policies and procedures that support the prevention of—and specify steps to be taken in the event of—a data breach. This should include procedures to notify authorities, parents, and other community members.
- Educate district staff about online educational services (paid and free) and how to determine whether they comply with FERPA and state and district regulations.
- Coordinate an annual privacy training for all school and district employees who have access to personally identifiable student data, adopt online educational services or apps, or procure and contract with service providers.
- Ensure that all third-party vendors that collect or have access to student data have written contracts that specifically address privacy and the allowable uses of personally identifiable information and prohibit further redisclosure of personally identifiable information without parental consent.
- Communicate directly with parents about the collection and use of student data and the privacy measures and protections that are in place to prevent confusion and misunderstanding.

- Prior to using online educational services, ensure that the contract or "terms of service" contain all necessary legal provisions governing access, use, protection, and destruction of student data.
- Ensure that agreements with outside providers include provisions allowing direct parental access to personally identifiable student information and assistance to schools for indirect parental access to other student data.
- Ensure greater transparency by posting on district and school websites all policies governing the outsourcing of school functions and contracts with outside providers.
- Make available a list of online educational services or apps that are used within the district.

Recommendations for School Leaders

- Familiarize yourself with FERPA, state, and district regulations concerning student data privacy.
- Communicate district policies related to student data collection and usage to your teachers and parents.
- Ensure that your teachers have been educated about the use of online educational services and how to determine whether they comply with FERPA and state and district regulations.
- Clearly communicate third-party vendors' privacy, security, and breach and indemnification policies to parents about personally identifiable information that is shared with those vendors.