POSITION STATEMENT: STUDENT DATA PRIVACY

PURPOSE

To provide policy recommendations to ensure the protection of student privacy and appropriate use of student data to improve teaching and learning in the classroom.

ISSUE

Data-driven decision-making has become a tenet of high-performing schools and is essential to transforming teaching and learning in the classroom. The Alliance for Excellent Education says that the "effective use of data and learning analytics are both critical components of a digital learning strategy to personalize learning for many more students, especially to increase student retention and achievement in the highest-need schools (page 2)." Narrowing achievement gaps and assisting all students to be college and career ready upon high school graduation have economic implications as well. In a report examining the potential of the use of data in education, the McKinsey Global Institute estimates "the potential value from improved instruction to be $310 billion to $370 billion per year worldwide, largely through increased lifetime earnings (page 22)."

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 the teaching and learning process, this must be done within parameters that protect the privacy of students and ensure that their data is used only for legitimate educational purposes.

While the collection and analysis of student data is essential to the teaching and learning process, this must be done within 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 US Department of Education approved new regulations clarifying that third-party vendors (such as those who help manage school databases or provide digital curriculum) can be included within the school official 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. Overall, 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, have become outdated in the new digital age.

In 2014, a congressional hearing was held to address student data privacy issues and a Senate bill was introduced to update FERPA and clarify that third parties are forbidden from using student information for marketing and advertising purposes. Fourteen states also enacted laws to strengthen student privacy protections, and the National Conference of State Legislatures reports that more than 100 student privacy bills were introduced in 36 states. Each principals' 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.

GUIDING PRINCIPLES

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.

POSITION STATEMENT: STUDENT DATA PRIVACY

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—a fundamental tenet of the Breaking Ranks framework for school improvement.

RECOMMENDATIONS

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.

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

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 District 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 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 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 preempt 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.

Ensure that principals receive training on policies and procedures that support 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

POSITION STATEMENT: STUDENT DATA PRIVACY

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.

RESOURCES

- Alliance for Excellent Education (June 2014). *Capacity enablers and barriers for learning analytics: implications for policy and practice*. Retrieved from http://all4ed.org/wp-content/uploads/2014/06/LearningAnalytics.pdf.
- Data Quality Campaign. (July 2014). *Getting the facts straight about education data*. Retrieved from http://dataqualitycampaign.org/files/Safeguarding Data - Getting Facts Straight.pdf.
- iKeepSafe. (2014). *Student data privacy and security: a roadmap for school systems*. Retrieved from http://storage.googleapis.com/iks/Roadmap.pdf.
- Krueger, Keith R. (June 2014). *10 steps that protect the privacy of student data*. The Journal. Retrieved from http://thejournal.com/articles/2014/07/23/10-steps-that-protect-the-privacy-of-student-data.aspx.
- McKinsey Global Institute. (October 2013). *Open data: unlocking innovation and performance with liquid information*. Retrieved from http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information.
- National School Boards Association. (April 2014). *Data in the cloud*. Retrieved from http://nsba.org/sites/default/files/reports/DataInTheCloud_Guide_NSBA_COSA.pdf.
- Parent Coalition for Student Privacy. (July 23, 2014). *Letter to member of Congress*. Retrieved from http://www.studentprivacymatters.org/wp-content/uploads/2014/07/Parent-Coalition-for-Student-Privacy-Letter-to-Congress-7-22-14.pdf.
- Reidenberg, J., Russell, N., Kovnot, J., Norton, T., Cloutier, R., & Alvarado, D. (2013). *Privacy and cloud computing in public schools*. Center on Law and Information Policy.
- US Department of Education Privacy Technical Assistance Center. (February 2014). *Protecting student privacy while using online educational services: requirements and best practices*. Retrieved from http://ptac.ed.gov/sites/default/files/Student Privacy and Online Educational Services (February 2014).pdf.
- US Department of Education Privacy Technical Assistance Center. (July 2014). *Transparency best practices for schools and districts*. Retrieved from http://ptac.ed.gov/sites/default/files/LEA Transparency Best Practices final.pdf.