POSITION STATEMENT: STUDENT DATA PRIVACY 2021

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.

Data-driven decision making has become a tenet of high-performing schools and is essential to transforming teaching and learning in the classroom. The Data Quality Campaign states that "data is one of the most powerful tools to inform, engage, and create opportunities for students along their education journey." While using data to personalize learning helps increase student retention, it also serves to narrow achievement gaps and assists all students to be college and career ready upon high school graduation. Recent studies from Louisiana State University found that "data-driven instruction also creates a more supportive and constructive school culture. It stops placing blame on the student for a lack of comprehension and instead creates a more supportive environment where students and teachers share responsibility. As a result of this dynamic, students feel supported and encouraged to succeed."

Technology has made it easier for principals and teachers to collect and analyze data at the school level, and many districts and states possess or are 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. 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 parental 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 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 collected from applicable surveys will be used for marketing purposes and provide an opportunity to opt out of the marketing; and the Children's Online Privacy Protection Act (COPPA) requires consent before operators of certain online services may collect, use, or disclose 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. These concerns continue to grow as more students have access to and are using digital tools to enhance their learning experiences.

Congress has held numerous hearings and introduced several bills on student data privacy since 2014, including bills updating FERPA and clarifying that third parties are forbidden from using student information for marketing and advertising purposes. However, none of these efforts have resulted in an update to current federal student data privacy laws or regulations. States have been much more active in introducing and passing student data privacy laws. From 2013–19, 45 states enacted 128 laws regulating student data privacy, with an additional five laws passing. Many of these laws fall into one of five of the following groups, according to the 2019 State Student Privacy Report Card released by the Parent Coalition for Student Privacy:

- Laws modeled after California's 2014 law known as the Student Online Personal Information Protection Act (SOPIPA). SOPIPA "prohibits operators of online educational services from selling student data and using such information to target advertising to students or to amass a profile on students for a noneducational purpose. The law also requires online service providers to maintain adequate security procedures and to delete student information at the request of a school or district" (Herold).
- Laws patterned after the Foundation for Excellence in Education's 2015 model bill, the Student Data Privacy, Accessibility, and Transparency Act, which provides extra protections to ensure student data is used responsibly by placing restrictions on data use on data collected by federal and state governments. Additional restrictions are placed on vendors as well.
- Laws that established access and security standards for state longitudinal data systems, while also authorizing state education departments to collect and share personal student data among several state agencies.

- Laws that prohibit the collection or disclosure of Social Security numbers, biometric, or other especially sensitive personal student information.
- Laws that regulate schools' access to students' social media accounts.

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.

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 Building Ranks™ framework for school improvement. NASSP also believes data is most valuable when each student has equitable access to digital tools or resources used to collect student data.

RECOMMENDATIONS

Recommendations for Federal Policymakers

- Review federal laws, such as FERPA and COPPA, and their intersection with state laws and regulations on the use of student data to ensure they balance privacy protection with the need to improve teaching and learning.
- Ensure additional funds and resources are provided to schools and districts for professional development to help educators ensure compliance with new laws and regulations.
- 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 funding for the U.S. Department of Education's Student Privacy Policy Office and Privacy Technical Assistance Center to develop guidance and provide technical assistance to states regarding the collection, storage, security protections, and destruction of student data.
- Pass legislation that provides states and school districts with adequate resources to put in place the necessary cybersecurity measures to protect 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.

- Continue to ensure that personal information and online learning activities are not used to target advertising to students or their families.
- Strengthen prohibitions on nonconsensual access to personally identifiable student data where access is limited to school, district, or state educational agency employees and to authorized service providers under their direct control and solely for the authorized educational purpose.
- Pass policies or regulations that ensure equitable access to digital tools and resources used to collect student data to ensure that data collected is up to date and features information on underserved populations.

Recommendations for State Policymakers

- If not already established, require the development of 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 state education agencies, 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 and ensure they have the resources to develop guidance and provide technical assistance.
- Develop policies on data collection, security, 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.
- Provide funding and resources to schools and districts to ensure they are capable of meeting the state-level requirements for protecting student data.

Recommendations for District Policymakers

- Develop clear policies about what student information is collected and for what purpose, how that data is secured and stored, to whom the data is disclosed, and each party's responsibilities in the event of a data breach.
- Ensure that data security practices include appropriate data retention periods, 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 and cybersecurity.
- 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.
- Develop and execute controlled procurement processes that ensure all proposed technology undergoes an internal vetting and approval process.
- 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 commercial use of student data and further redisclosure of personally identifiable information without consent.
- Clearly communicate directly with parents about the tools in use in the district, 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 requiring either parental access to personally identifiable student information or assistance to schools for indirect parental access to 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, COPPA, state laws, and district regulations concerning student data privacy.
- Clearly communicate district policies and roles related to student data collection, usage, and cybersecurity to your teachers, other relevant staff, school board, and parents.
- Ensure that your teachers have been educated about the appropriate use and processes applicable to adopting 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.
- Ensure that instructional decisions made from collected data are evidence-based and done so in a manner that best prepares a student for success in their education.

RESOURCES

- Data Quality Campaign. (2020, August 11). Maintaining trust as data use changes. Retrieved from https://dataqualitycampaign.org/resource/student-data-privacy-and-the-covid-19-crisis/
- Data Quality Campaign. (2020, August 11). Supporting students while learning at home: Individual student data and the COVID-19 crisis. Retrieved from https://dataqualitycampaign.org/resource/individual-student-data-and-the-covid-19-crisis/
- Data Quality Campaign. (2015, April 29). The federal role in safeguarding student data. Retrieved from https://dataqualitycampaign.org/resource/federal-role-safeguarding-student-data/
- Fitzgerald, D. (2018, December 13). Why education data? Retrieved from https://dataqualitycampaign.org/why-education-data/.
- Fritchen, K. (2020, January 09). The trouble with student data privacy laws. Retrieved from https://securityboulevard.com/2020/01/the-trouble-with-student-data-privacy-laws/
- Gallagher, K., Magid, L., & Pruitt, K. (n.d.). The educator's guide to student data privacy. Retrieved from https://www.connectsafely.org/eduprivacy/
- Grant-Chapman, H. (2020, November 30). Three lessons from COVID-19 and the changing landscape of student privacy. Retrieved from https://cdt.org/insights/three-lessons-from-covid-19-and-the-changing-landscape-of-student-privacy/
- Herold, B. (2014, September 30). "Landmark" student-data-privacy law enacted in California. Retrieved from https://www.edweek.org/technology/landmark-student-data-privacy-law-enacted-in-california/2014/09
- Kerry, C., Morris, J., Chin, C., & Turner-Lee, N. (2020, June 03). Bridging the gaps: A path forward to federal privacy legislation. Retrieved from https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/
- Laird, E. (2019, January 30). Chief privacy officers: Who they are and why education leaders need them. Retrieved from https://cdt.org/insights/chief-privacy-officers-who-they-are-and-why-education-leaders-need-them/
- LSU Online. (2020, June 11). How educators can use student data to drive instruction. Retrieved from https://online.lsu.edu/newsroom/articles/how-educators-can-use-student-data-drive-instruction/
- Parent Coalition for Student Data Privacy. (2019, January). The state student privacy report card. Retrieved from https://www.studentprivacymatters.org/state-legislation/
- Quay-de la Vallee, H. (2019, March 14). Balancing the scale of student data deletion and retention in education. Retrieved from https://cdt.org/insights/balancing-the-scale-of-student-data-deletion-and-retention-in-education/
- Ritvo, D. T. (2016 June). Privacy and student data: An overview of federal laws impacting student information collected through networked technologies. Cambridge, MA: Cyberlaw Clinic, Berkman Center for Internet & Society at Harvard University.

- Roscorla, T. (2016, March 24). 3 student data privacy bills that Congress could act on. Retrieved from https://www.govtech.com/education/k-12/3-Student-Data-Privacy-Bills-That-Congress-Could-Act-On.html
- Solari, J., Tay, A., Gray, E., Lemke, R., Cottrell, S., & Sellers, J. (2020, January). How to engage and train stakeholders regarding privacy and security best practices. Retrieved from https://slds.ed.gov/#communities/pdc/documents/18506
- Student Privacy Compass. (2020, December 1). Education during a pandemic: Principles for student data privacy and equity. Retrieved from https://studentprivacycompass.org/pandemicprinciples/