Policy Brief | August 2016

Policy analysis from SREB's 10 Issues in Educational Technology

SREB

Data Privacy and Security

Educational technology systems generate enormous amounts of data, which allow schools and colleges to provide more personalized services to every student. Creating a culture of efficient data use for students is critically important, but equally important is securing the data collected from these systems. Data privacy and security cannot be a "behind the scenes" approach for education agencies; risk assessment and mitigating practices should be common knowledge and inherent in the culture of effective data use.

Although data privacy and security go hand in hand, they are two different concepts. Data security involves the technical and physical requirements that protect against unauthorized entry into a data system and helps maintain the integrity of data. Data privacy is about data confidentiality and the rights of the individual whom the data involve, how the data are used and with whom data can legally be shared.

Without clear policy, the concerns of the stakeholders cannot be fairly balanced in the best interests of students, their achievement, and effective and efficient educational decision-making.

Data Value and Use

Educators have long relied on research and data to identify effective teaching and learning strategies. As innovative instructional models have emerged, tailored instruction has the potential to improve and accelerate student learning, as well as focus on individual needs and skills. This personalized learning approach is possible because of technological advancements that permit data to be gathered from various systems and analyzed. Such data can inform educators of students at risk of falling behind, identify a more effective path of learning, verify student achievement and specific needs, and inform educators of needed resources.

Inside

This policy brief is one of several forthcoming briefs on SREB's Educational Technology Cooperative's 10 Issues in Educational Technology. This report covers two issues, Data Privacy and Technology Security. The remaining issues to be featured are: Data Systems, Predictive Analytics, Bandwidth, Emerging Technologies, New Learning Models, Student Digital Literacy, Digital Accessibility, and Policy.

Southern Regional Education Board

SREB.org

Policymakers and administrators have depended on access to accurate data to identify critical education issues, gauge progress and assess policy implementation. In today's digital world, electronic data offer greater promise for informing policy. At the same time, data require more secure systems to guard against breaches, and data managers require better training to ensure privacy, especially of students and teachers. The balance between security and privacy on the one hand and access to data on the other is tenuous.

Privacy and Security Risks

In recent years, public concern about data privacy and security has primarily been due to security breaches. According to the PrivacyRights.Org database, 54 breaches affecting more than 1.1 million records have occurred in educational systems since 2014. The variety of breaches this year (through June 2016) in K-12 include: student ID numbers used in a vendor system, student information sent to the wrong individuals, students accessing records without permission, employee social security numbers publicly released with salary data, and a breach that disclosed social security numbers and tax information due to unauthorized access to employee W-2 forms. At the university level, the breaches this year include: unauthorized access to financial records, medical records, grades and social security numbers; a cyber-attack on a human resources system that contained W-2s and banking information; and vulnerabilities to data storage systems owned by a third party vendor. These breaches are publicly known; however, other breaches may have gone unnoticed or undisclosed.

789%

"According to a recent PhishMe analysis of phishing email campaigns (for example, deceptively posing as a reputable entity via email), during the first three months of 2016, there were 6.3 million more phishing attacks than there were during the same period last year. This represents a 789 percent increase primarily due to an upsurgence in ransomware."

— Source: eSchool News, June 8, 2016

In December 2015, the University of Connecticut disclosed a breach when malware was found on its website "prompting visitors to download a malicious program posing as Adobe Flash Player," according to a university spokesman.

In January 2016, Southern New Hampshire University began investigating accidental exposure of a student database. "The database contained more than 140,000 records, including students' names, email addresses, IDs, course names, course selection, assignment details, assignment scores, and instructors' names and email addresses." The university stated a third party vendor was responsible for the error.

In February 2016, hackers demanded a ransom of $10,000 in bitcoin to get an encryption key to the district computer system for Horry County Schools in South Carolina. Ransomware attacks, use of high-level encryption of data in which the encryption key is only provided upon payment of the ransom, are on the rise and affecting schools, health care systems and government entities.

Security risks from such breaches, whether from hacking, malware, ransomware, third party system vulnerabilities or employee mistakes, have heightened public concern. Policymakers have been prompted to act to ensure student and employee privacy and protection.

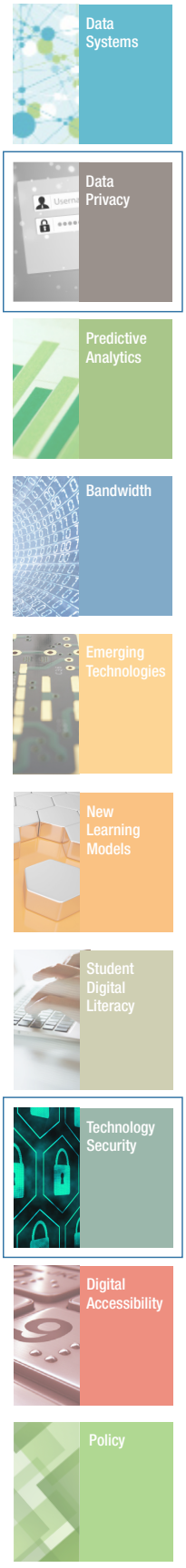
Legislative Actions

The 1974 Family Educational Rights and Privacy Act (FERPA) provides parental access to education records and opportunity to have those records amended. It also offers some control over the disclosure of information in student records. Although the content of student records has changed drastically in recent years, these provisions govern the management of education records across states. In response to the aging foundation of federal law, in recent years, states have enacted legislation to better reflect the complexity of today's data, technology systems, collaborative partner or vendor relationships, cloud initiatives and security risks.

In 2013, Oklahoma became one of the first states to enact legislation to address student data privacy and security. Other states quickly followed its lead. Between 2013 and 2015, more than 300 bills addressing education data privacy and security were introduced in state houses nationwide. These bills sought to address specific education data privacy and security issues, including data governance, processing, storage, collection, sharing and transparency. In all, 34 states — including 14 SREB states — enacted education data privacy and security laws from 2013 to 2015. While these state laws are not identical in nature, they share similarities. The most comprehensive state laws are outlined in Table 1, which provides frequencies for some common elements of data privacy legislation.

TABLE 1: Highlights of Data Privacy Legislation in SREB States

Highlights of Recent Data Privacy Legislation	AR	DE	FL	GA	KY	LA	MD	NC	OK	SC	TN	TX	VA	WV
Comprehensive laws regarding handling and protection of student data		✓		✓			✓		✓					✓
Inclusion of parents' rights to access student information			✓	✓		✓		✓						
Specification of assuring FERPA compliance								✓		✓			✓	✓
Designation of official state position to be filled by a person who will oversee data security, privacy and governance				✓									✓	✓
Prohibition of selling student data or using it for advertising	✓	✓			✓		✓							
Prohibition of collection of biometric information on students	✓		✓						✓					
Prohibition on use of social security numbers			✓						✓					
Mandate creation of unique student identification numbers			✓			✓								
Limits placed on data sharing within the state						✓								
Limits placed on data sharing outside of the state									✓					
Confidentiality of student records and redaction												✓		



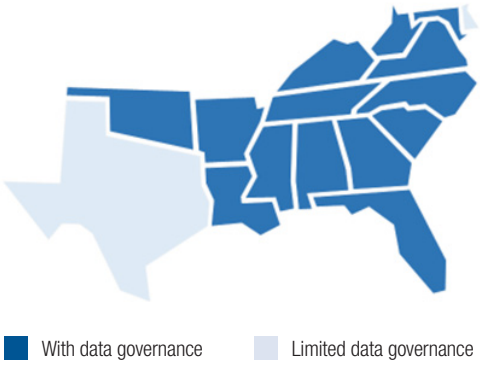
Georgia used ExcelinEd's Student Data Privacy, Accessibility and Transparency Act as the basis for Senate Bill 89, which passed unanimously in both chambers of the legislature. The model policy enhances federal privacy protections and aligns with international privacy best practices.

Data Governance

Other data privacy and security concerns have been fueled in part by a perceived lack of transparency about how, when and where data are collected, used and made available. If data management is not transparent, it is hard for students, parents and other constituents to trust its accuracy and utility.

Data governance policies should address transparency, privacy, collection, use and sharing. It should also ensure the primary purpose of data should be for improving student learning. Governance policies should be in place to protect the privacy of the student and employee, such as de-identifying data and ensuring a large enough sample so that individuals cannot be surmised from the data. Permission to access data should be role-based so sensitive data is only available for specific stakeholders. Transparency about who is responsible for securing the data, as well as transparency about the policies and procedures for security are important. Compliance audits should be an integral part of governance, and pass/fail rates of agencies or systems should be publicly available.

FIGURE 1: SREB States With Data Governance by the State Board of Education



Source: Education Leaders Report Vol. 2, , No. 1, April 2016

As states pass new laws, policymakers should monitor implementation to ensure their states strike the balance between security, privacy and access. If the scale tips, states need mechanisms to correct the balance. In 14 SREB states, state boards of education have rule-making authority on data governance — making it easier for boards to adjust policies as needed. In two SREB states, boards have some rule-making authority but are limited to issues designated by their legislatures. Recent laws in some states lean toward state board of education or state education agency governance. These state agencies can ensure data accuracy by working with local education agencies on data outliers. State education agencies have the ability to oversee implementation of new data policies and practices through the local agencies. They have the authority to require training of data users; they also ensure that position descriptions reflect data handling responsibilities.

Recommended Policies

Current research and best practices provide states with clear recommendations for data-related policies. Legislation, policies and best practices should include: documented processes, transparency of use, effective communication, review and enforcement of security practices, sufficient ongoing training of personnel, sufficient staffing of IT and support personnel, and a commitment to protect the integrity and authorized use of student data.

Transparency

State policy needs to clarify data governance for P-20 education data collection, access, sharing and security. It should ensure strong communication that informs the public, especially students and parents, about current policies and proposed changes. Policy should also specify notification processes for misuses of data and data breaches.

Information about data policies should be easy for the public to find — not buried on websites. The text should be concise and easy to read, without jargon. It should indicate how data are collected, shared and used, who has access, and what safeguards protect student privacy. In 2016, the National Association of State Boards of Education reported that Colorado, Louisiana, West Virginia and Wisconsin increased transparency on state education privacy policies with methods that respectively included fact sheets, a state guide, statewide forums and a well-designed, privacy-focused website.

Role-based Usage Permissions

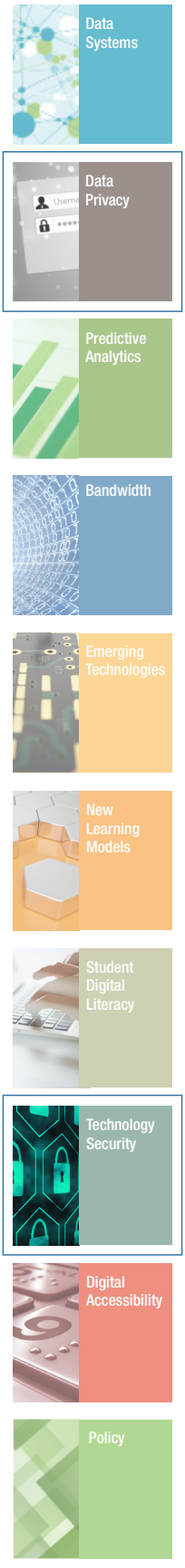
Policymakers use data for decision-making, funding and predictive modeling of student outcomes to improve education systems, processes and policy. Teachers use data to inform best practices, to find where students are falling behind, to target instruction on specific needs or skill sets, and to help students with troublesome concepts that require more class time. Parents use data to follow the progress of their children, to intervene if problems arise, and for opportunities to accelerate learning. Each role requires different types of access and permissions. Data dashboard displays can be customized by user role to make interpretation of data more clear and access to information more intuitive. Charts and graphs for comparison of data tend to be easier to understand for stakeholders than numbers in a table. Predictive analytics for student outcomes and at-risk students can be more easily interpreted through dashboards so instructor interventions can be timely and targeted. By defining and making public the various roles, permissions and uses of data, policymakers improve transparency and increase public trust.

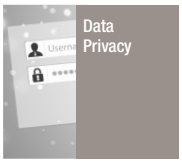
Monitoring and Breach Notification

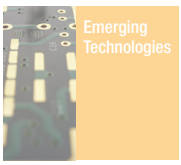
State boards of education and higher education agencies should ensure that local educational systems' actions reflect systems' responsibilities to use data effectively, train data users and protect the systems that contain and transmit data. They also have the responsibility to ensure adequate funding for multi-layered security systems, security audits, and IT staff to collectively monitor data systems and circumvent security breaches. Any server or device with potential for public access could be a point of breach, and considering the number of devices per person used on a daily basis, adequate security systems and staffing is critical.

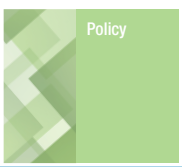
> Vendor technology systems can contain communication between students and teachers, grades, feedback on homework and assignments, and personally identifiable information.

Timely notification of security breaches is important for public trust. It is improbable to expect that breaches to data systems will ever end, even though that is the goal. But delays in notifying users about breaches puts them at more risk, especially if users repeat the same passwords in multiple systems. Prompt notification allows users to proactively change passwords across various applications. It also prompts them to consider credit monitoring or identity-theft protection if social security numbers or tax information is compromised. The National Conference of State Legislators provides information on the 47 states that have security breach notification laws.









State board policies should include detailed plans for responding to security breaches, including notifications of users affected or potentially affected, remediation to correct the problems and related procedures to mitigate risks. Policies should address vendor data systems, procedures for safe data transmission and notification of vendor system breaches. Proper staff training for steps to take in the event of a breach is also critical.

Training

Maryland and Virginia have comprehensive data privacy training requirements for education personnel. These policies ensure that personnel who have access to student data know how to secure, protect and use it effectively and ethically. IBM reports that human error is a factor in 95 percent of data security incidents. Experts say many data breaches could be avoided if personnel were properly trained and supervised. Yet, school-level data are all too often entered by employees with little training.

> 95 percent of data security incidents are due to human error.
>
> — *IBM*

Education agencies with new data systems provide training on the many benefits of data for educational achievement, but training requirements should include awareness of risks in data management, consequences of accidental disclosure, required practices in the event of a data breach, best practices in data privacy to de-identify data, and security based on the roles and permissions of users. Instructors should be trained on FERPA, state data laws, and local data policies and practices. Training should be ongoing and required for all data users, with targeted information based on their user roles.

Technical Support

Effective data use for new systems requires a comprehensive implementation plan and a project coordinator to oversee implementation throughout school districts and institutions. Existing systems require maintenance and upgrades, especially as security risks evolve. Staff turnover requires role and permission setups, granting appropriate access to the data systems, training on effective use, troubleshooting and general technical support for using data systems. Constant changes in technology and regulatory compliance require frequent upskilling of IT staff. Policymakers should recognize the support functions required to make education data systems both useful and secure, and provide adequate funding for technology staff, systems, tools and training.

Conclusion

Finding the right balance between data privacy and security concerns and meeting individual student educational needs is difficult. Educational technology systems can provide data to personalize students' paths to achievement — a highly desirable outcome. After all, learning does not happen in the same way or at the same pace for all students. And no classroom can meet every child's needs. But for such educational technology systems to work fairly and ethically, states should provide the necessary resources to protect them from unauthorized access, use, disclosure, disruption, modification and destruction, while keeping them highly available for learning. Transparent policies about data collection, access, security monitoring and notification of breaches are imperative to keep the public trust. Balancing security with effective use and privacy of data is worth the effort for improving student outcomes and meeting the mandate of the public that their individual privacy is protected.

References

Data Quality Campaign. (2015, May). *Student Data Privacy Legislation: What Happened in 2015, and What Is Next?* Retrieved from Data Quality Campaign website http://www.dataqualitycampaign.org/resource/student-data-privacy-legislation-happened-2015-next/

Data Quality Campaign. (2016, May). *Safeguarding Data*. Retrieved from Data Quality Campaign website http://www.dataqualitycampaign.org/topic/safeguarding-data/

ExcelinEd.org. (2016, May). *Model Legislation*. Retrieved from ExcelinEd website http://www.excelined.org/wp-content/uploads/Student-Data-Privacy-Accessibility-and-Transparency-Act-Model-Legislation-03.2015.pdf

FerpaSherpa.org. (2016) *Foundation for Excellence in Education Privacy Toolkit*. Retrieved from Ferpa Sherpa website https://www.ferpasherpa.org/foundation-for-excellence-in-education-privacy-toolkit/

McCrea, B. eSchool News. (2016). *How Hackers Held a District Hostage for Almost $10,000*. Retrieved from eSchool News website http://www.eschoolnews.com/2016/06/08/how-hackers-held-a-district-hostage-ransomware/

National Association of State Boards of Education. (2016, May). *2015 State Legislation: Education Data Privacy*. Retrieved from NASBE website http://www.nasbe.org/wp-content/uploads/2015-State-Legislation-6-9.pdf

National Conference of State Legislators. (2016, June). *Security Breach Notification Laws*. Retrieved from NCSL website http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Privacy Rights Clearinghouse. (2016, June). *Chronological Database of Data Security Breaches*. Retrieved from Privacy Rights Clearinghouse website http://www.privacyrights.org/data-breach

Southern Regional Education Board. (2016, May). *Gauging Progress, Accelerating Pace*. Retrieved from SREB website http://www.sreb.org/goals-and-state-progress-reports

U.S. Department of Education. (2010). *Use of Education Data at the Local Level: From Accountability to Instructional Improvement*. Retrieved from U.S. Department of Education http://www2.ed.gov/rschstat/eval/tech/use-of-education-data/index.html?exp=0

Vance, A. (2016, May). National Association of State Boards of Education. *Policymaking on Education Data Privacy: Lessons Learned*. Retrieved from NASBE website http://www.nasbe.org/wp-content/uploads/NASBE-Policy-Update-2015-Legislative-Session-Data-Privacy_-June-2015.pdf

This report was prepared by Wanda Barker, director, Educational Technology Cooperative, Jeff Gagne, director, Policy Analysis and Joan Lord, vice president for Education Data, Policy Research and Programs, with research support from former policy analyst Caitlin Daugherty. For more information, email Wanda.Barker@SREB.org.

SREB

Southern Regional
Education Board

Southern Regional Education Board
592 10th St. N.W.
Atlanta, GA 30318-5776
(404) 875-9211

www.SREB.org

August 2016 (16T02)