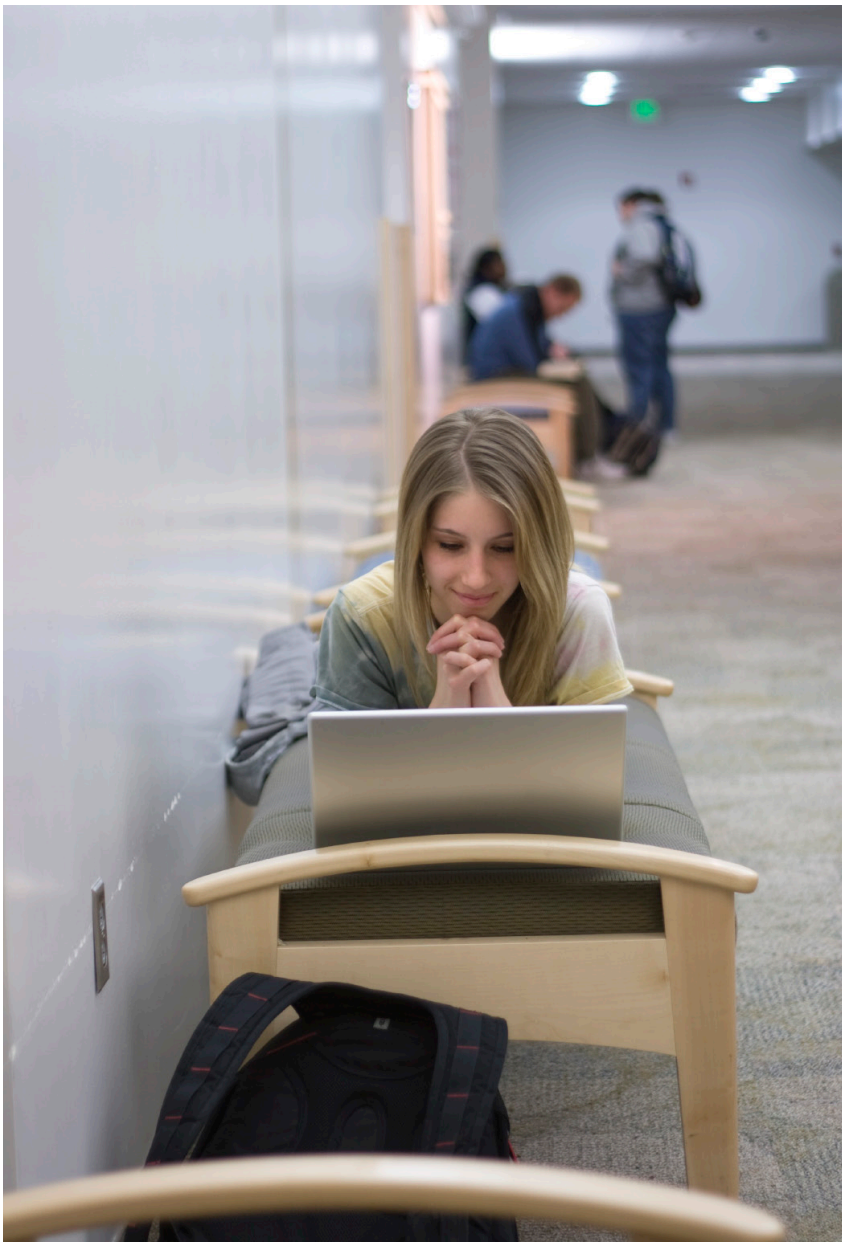
NCSL

Connected Learning: A Primer for State Policymakers

Third of four reports

Protecting Student Privacy in a Networked World



BY SUNNY DEYE

The digital revolution is changing the way people learn. Understanding how to interact with the digital tools, networks and social media platforms of the Internet is critical to the 21st century learner. Learning environments—including schools, libraries, museums and community centers—are upgrading technology so young people can access digital tools throughout the day, creating new opportunities to learn any time, any place and at any pace.

Throughout 2014, the Aspen Institute Task Force on Learning and the Internet—a group of 20 innovative and respected minds in technology, public policy, education, business, privacy and safety—studied the ways young people learn today. They found that, for 21st century learning environments to fully take advantage of the opportunities provided by the Internet, they also must resolve serious issues of trust, safety, privacy, literacy and equity of access. Among other recommendations, the task force found that the best approach to establishing trusted online learning environments is to have all stakeholders—including learning professionals, civic officials, local associations, parents, teachers, students and businesses—collaborate in setting local, state and/or national student privacy standards.

Policy Considerations—Student Privacy

As networked learning environments become increasingly prevalent, there is a growing need to assure students, parents, educators and policymakers that information about individual students and their learning is collected properly and used appropriately. State policymakers recognize the value of data to provide critical information about individual student and educator performance, as well as information about what is working, what might be improved, and what information is needed to empower parents, educators and others who have a stake in education to help students succeed. They are addressing a variety of issues related to student privacy, recognizing that participation in trusted online learning environments provides a variety of digital skills and competencies that now are basic to classroom performance, workforce readiness and full participation in civic life.

State Policy Approaches

States are addressing student privacy through a variety of policies, including creating governance structures to oversee transparency, protecting the privacy of student data, and prohibiting specific uses and sharing.

CALIFORNIA

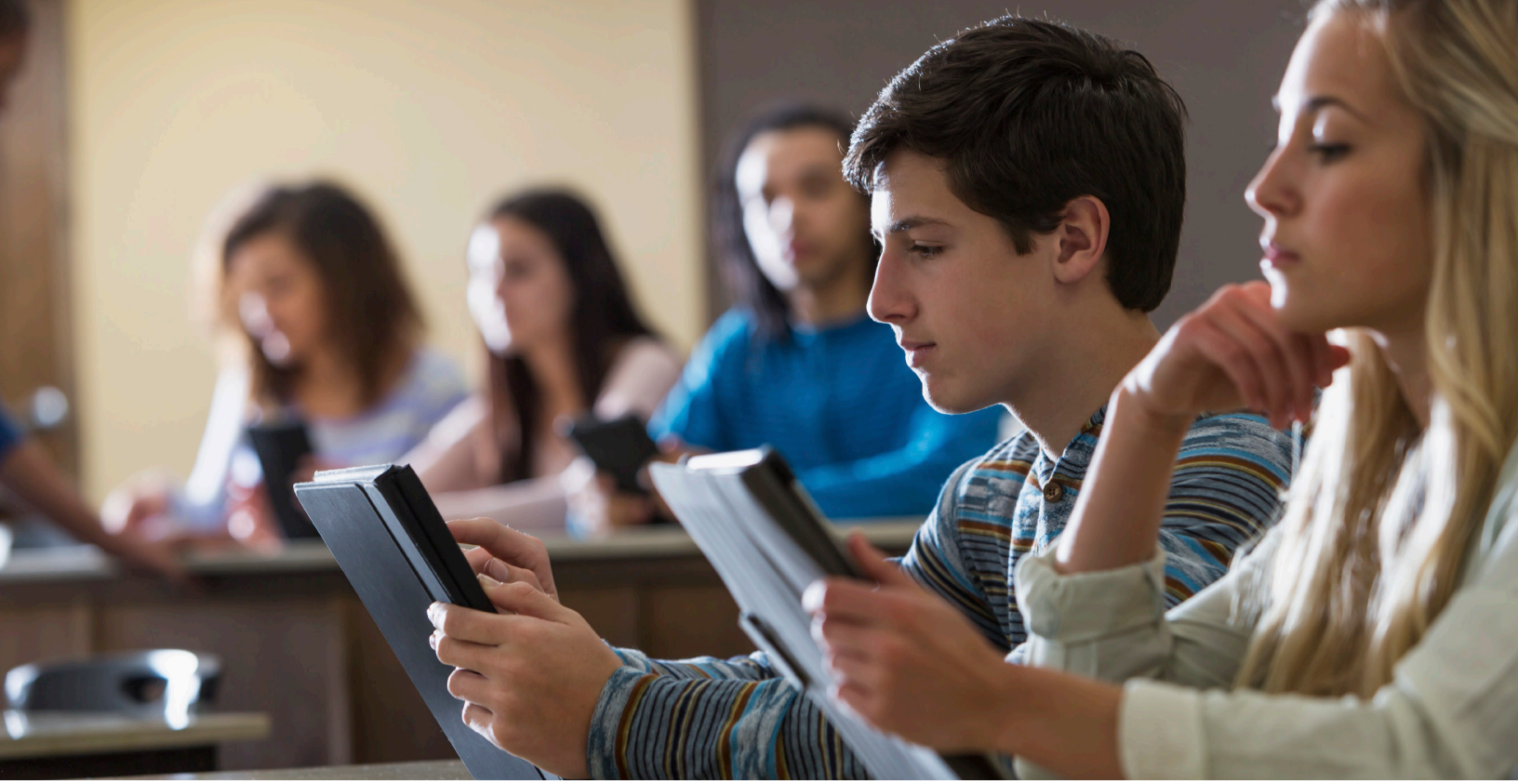
- **SB 1177** (2014), the Student Online Personal Information Protection Act, prohibits an operator of a website, online service, online application or mobile application from knowingly engaging in targeted advertising to students or their parents or legal guardians. These services and applications also may not use covered information to amass a profile about a K-12 student, sell a student's information or disclose covered information. The law also addresses security procedures and practices of covered information in order to protect information from unauthorized access, destruction, use, modification or disclosure.

COLORADO

- **HB 1294** (2014), the Student Data Privacy Act, requires the State Board of Education to publish an inventory of the individual student data currently in the student data system as required by state and federal education mandates, as well as any student data proposed for inclusion in this system. It prohibits the Department of Education from providing individual student data to other organizations or agencies outside the state except under specified circumstances.

IDAHO

- **SB 1372** (2014), the Student Data Accessibility, Transparency and Accountability Act of 2014, requires the State Board of Education to create, publish and make publicly available a data inventory that defines individual student data fields included in the student data system. The index must include any individual student data required to be reported by state and federal education mandates; any individual student data proposed for inclusion in the student data system with a statement explaining the reason for inclusion; and any individual student data collected or maintained with no current purpose or reason. The board is required to ensure



that any contracts that govern databases, online services, assessments or instructional supports that include student data and are outsourced to private vendors, include express provisions that safeguard privacy and security, contain the restrictions on secondary uses of student data, and provide for data destruction. The act also includes penalties for noncompliance.

NEW YORK

- **SB 6356** (2014) prohibits the Department of Education from providing personally identifiable information to service providers, calls for destruction of any data already provided and allows districts to opt out of providing students' personally identifiable information to any party for inclusion in a data dashboard. It also creates a new position of chief privacy officer, who must make security and privacy policy recommendations and develop procedures for transparency, notification and parent complaints; calls for a parents' bill of rights for data privacy and security and a data inventory; and lays out guidelines for contracting with service providers.

RHODE ISLAND

- **HB 7124** (2014) limits the use of student data and information obtained by cloud computing service providers when providing services to K-12 educational institutions. It also prohibits the use of such data for commercial purposes, including advertising that benefits the service provider.

WEST VIRGINIA

- **HB 4316** (2014) outlines state, district and school responsibilities for data inventory and provides for a data governance officer. It requires the State Board of Education to develop guidelines for school districts, requiring them to notify parents of their right to request student information and allow parents to access data specific to their child's educational record; ensure security when providing student data to parents; make sure student data is provided only to authorized individuals; and detail the timeframe within which record requests must be provided.

OKLAHOMA

- **HB 1989** (2013), the Student Data Accessibility, Transparency and Accountability Act, requires public reporting of which student data are collected by the state, mandates creation of a statewide student data security plan, and limits the data that can be collected on individual students and how that data can be shared. It establishes new limits on the transfer of student data to federal, state, or local agencies and organizations outside Oklahoma. It also restricts the state from requesting delinquency records, criminal records, medical and health records, social security numbers and biometric information as part of student data collected from local schools and districts.

UTAH

- **SB 82** (2013) provides access by a student's parent or guardian, or an authorized Local Education Agency (LEA) user, to the learning profile of a student from kindergarten through grade 12 in an electronic format known as a Student Achievement Backpack. It requires the State Board of Education to implement security measures to ensure that the data is secure and confidential and that an authorized LEA user may only access student data that is relevant to the user's LEA or school.

Student Privacy Pledge

A concurrent effort is being led by a growing number of school service providers who are signing the Student Privacy Pledge, a voluntary effort led by the Future of Privacy Forum and the Software and Information Industry Association. The pledge is designed to build trust by effectively protecting the privacy of student information and communicating with parents about how student information is used and safeguarded. By signing the Student Privacy Pledge, school service providers agree to safeguard student privacy through a series of commitments regarding the collection, maintenance and use of student personal information. The commitments are intended to detail ongoing industry practices that meet and exceed all federal requirements and to encourage service providers to more clearly articulate these practices to further ensure confidence in how they handle student data.

The pledge applies to all student personal information, whether or not it is part of an "educational record" as defined by federal law, and whether collected and controlled by the school but warehoused offsite by a service provider, or collected directly through student use of a mobile app or website assigned by a teacher. It applies to school service providers whether or not a formal contract exists with the school.

The pledge holds school service providers accountable to the following agreements to:

- Not sell student information
- Not behaviorally target advertising
- Use data only for authorized education purposes
- Not change privacy policies without notice and choice
- Enforce strict limits on data retention
- Support parental access to, and correction of errors in, their children's information
- Provide comprehensive security standards
- Be transparent about collection and use of data

To date, the Student Privacy Pledge has 131 signatories. Participating school service providers and the full language of the pledge is available online at www.studentprivacypledge.org.

Policy Questions to Consider

1. What is the purpose of the state's privacy policy? Legislation, such as Idaho's SB 1372 (2014), described on page 2, can express a commitment to education data privacy while acknowledging the educational value of effective data use.
2. Who is responsible for developing and overseeing privacy and security policies? States are selecting state leaders, advisory boards or other government structures to be responsible for ensuring privacy and security. For example, West Virginia's HB 4316 (2014) requires the state superintendent of schools to appoint a data governance officer as part of the state's Student Data Accessibility, Transparency and Accountability Act.
3. Which data is included in data governance policies? States are broadening their definitions to include early learning, K-12 and workforce data in their data governance policies.
4. What are privacy requirements for private companies providing digital services to students? California's SB 1177 (2014), described on page 2, applies to operators of K-12 Internet websites, online services, online applications and mobile applications, whether or not they contract with schools. The legislation clarifies that student data may be used only for school purposes. Providers are prohibited from using, sharing, disclosing or compiling personal information about students for commercial purposes, including advertising and profiling.

Considerations for State Policymakers

The state policy examples discussed here encompass a wide range of approaches to addressing the issue of student privacy in an increasingly networked world. As institutions such as schools, libraries, museums and community centers find new ways to increase access to learning opportunities, they must collaborate to develop expectations and guidelines that ensure proper and appropriate use of student data.

State legislators are leading the movement to embrace technology as a powerful learning tool, both in and out of school. Other briefs in this series explore how state legislatures are adjusting policies to harness the power of technology in the classroom, expand broadband access and promote digital literacy so that young people know how to communicate, collaborate and behave ethically online.

Recommended Resources

Learner at the Center of a Networked World is the 2014 report of the Aspen Institute Task Force on Learning and the Internet.

The Connected Learning Alliance is a network of organizations, projects and individuals working to make learning relevant by integrating personal interests, peer relationships and the tools of the digital age.

The Data Quality Campaign supports state policymakers and other key leaders to promote the effective use of data to improve student achievement.

Acknowledgments

This is the third publication in the NCSL Connected Learning series, exploring how the opportunities and realities of the digital age expand access to continuous learning for youth and adults. NCSL is grateful to the John D. and Catherine T. MacArthur Foundation for supporting this project and recognizing the critical role of state legislatures in education policy.

NCSL Contact

Sunny Deye
Education Program Principal
303-856-1469
Sunny.Deye@ncsl.org

NATIONAL CONFERENCE of STATE LEGISLATURES

William T. Pound, Executive Director

7700 East First Place, Denver, Colorado 80230, 303-364-7700 | 444 North Capitol Street, N.W., Suite 515, Washington, D.C. 20001, 202-624-5400

www.ncsl.org

 ISBN 978-1-58024-761-0