BELLWETHER
EDUCATION PARTNERS

PERSONALIZED LEARNING POLICY PLAY #14:
ENSURE THIRD-PARTY PROVIDERS ARE ABLE TO ACCESS THE DATA THEY NEED TO SUPPORT PERSONALIZED LEARNING, WHILE ALSO PROTECTING STUDENTS' PRIVACY AND FERPA RIGHTS

CONTEXT

Personalized learning models create a wealth of data about student learning and progress, and use this data to customize instruction and support to students' current skill levels, interests, and learning styles. This explosion of educational data has real potential to improve student learning outcomes, but it also creates new challenges. One such challenge involves the question of who owns student data and when and how schools or districts may share that data with third-party providers supporting personalized learning models. Schools, districts, and providers must be able to access and use the data they need to customize student learning experiences, but they must also protect student privacy.

Numerous state and federal laws exist to protect student privacy and ensure that student data are not shared inappropriately. These policies have been established in a piecemeal fashion over time, however, creating confusion for schools that want to implement personalized learning models. Recent controversies illustrate this challenge. District partnerships with inBloom, a nonprofit organization that used cloud-based storage to manage student data, led to parental concern that third-party providers may inappropriately share data with other external providers. After facing continued opposition from parents and school districts, inBloom decided to wind down its operations. Meanwhile, a group of nine plaintiffs, represented by the Electronic Privacy Information Center, recently sued Google for violating federal education privacy laws after the company admitted that it scans e-mails of students who use Google Apps for Education. In response, Google announced that it will no longer collect or use data from Apps for Education for advertising purposes.

States are beginning to pass data privacy bills, but these bills vary widely in their scope and the types of limitations they place on data sharing. Some are merely cosmetic and do little to protect student privacy. At the other extreme, poorly designed legislation could create major hurdles to implementing personalized learning models that use data to customize student learning experiences.

PLAY IN ACTION

To protect student privacy, states should require districts to develop clear guidance for providers and schools regarding access, use, and disclosure of student data. Charter school authorizers—both district and non-district—should adopt similar guidelines. A 2014 report from the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) provides guidelines on proper use and storage of data generated by digital learning resources. In addition, the Consortium for School Networking (CoSN), in partnership with Harvard Law School's Cyberlaw Clinic, released a toolkit in 2014 to help school systems navigate the privacy issues they face when using education technology. These guidelines are designed to provide broad recommendations for schools and districts, but district leadership will still need to establish specific policies based on local needs.

Both PTAC and CoSN recommend that schools and districts partnering with third-party providers create written contracts or legal agreements that clearly state the types of data collected and the purpose of collecting them. Contracts should also include specific provisions about data use and destruction, conditions for disclosing student information, and procedures in the event of a security breach. States can help by providing schools and districts with model contract language, which would be beneficial because existing district service contracts, such as those with transportation providers, do not typically address some of the crucial issues that emerge in partnerships with personalized learning providers. For example, contracts may need to discuss providers' rights and responsibilities in using or sharing metadata—information that provides additional meaning to collected data (for example, the number of times a student attempts to answer a question before responding correctly). PTAC's guidance emphasizes that providers should use these contextual data only for the purposes for which they were received. (Google's potential use of student metadata was a key issue in the lawsuit regarding the company's Apps for Education.)

PTAC also recommends that schools and districts be as transparent as possible with parents and students about what data are being collected, who has access to them, and how they may be used. Districts should

annually inform parents and students about their student data collection and privacy policies, as well as parents' rights, and publish this information online. This transparency will allow parents to fully understand school standards regarding technology and privacy, as well as their rights in relation to their child's personal information.

IMPLEMENTATION CONSIDERATIONS

One key challenge to creating state and local policies regarding student privacy is ensuring these policies align with the Federal Education Rights and Privacy Act (FERPA). FERPA was established in 1974, before the era of digital learning. As a result, education stakeholders today have different opinions on how students' personally identifiable information should be protected from third-party providers. Although FERPA restricts schools from releasing student data without parental or student consent, the law has several exceptions that schools and providers can leverage. For instance, the school official exception allows schools to release student data to a third-party provider if the provider meets criteria—set by the school's or district's annual FERPA notification—for being a school official with a legitimate interest in student education records. Because diverse stakeholders may interpret these exceptions differently, districts should create clear standards for schools partnering with third-party providers.

Schools should maintain ultimate control over student data. This will prevent outside providers from using student data for unauthorized purposes such as targeted advertising. In an example discussed in the PTAC guidelines, a provider managing a school's cafeteria account services may have access to student names and other data to create an online system for students and parents. This provider may not, however, use these data to create targeted food advertising directed at the same students.

In creating or revising policies on data and student privacy, districts should make sure they do not create conditions that are overly restrictive for schools and providers. For schools to serve students as effectively as possible, they must have access to improved technology, and this technology depends on the use of data to personalize instruction for each student. Districts should not be so cautious that they create barriers to the implementation and use of effective personalized learning models that have the potential to dramatically improve student performance.

CONTACT FOR ADDITIONAL INFORMATION

Karen Cator, Digital Promise:
karen@digitalpromise.org

RESEARCH AND RESOURCES

A *New York Times* article on the **controversy** related to **inBloom** and the company's decision to wind down operations is available at: http://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/

Read about the **lawsuit Google** faces regarding its **Apps for Education** at: http://www.theguardian.com/technology/2014/mar/19/google-lawsuit-email-scanning-student-data-apps-education

Read **Google's** announcement about its **new privacy policies** for Apps for Education at: http://googleenterprise.blogspot.com/2014/04/protecting-students-with-google-apps.html

The **federal PTAC report** on protecting the privacy of students using **online educational services** is available at: http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf

An *Education Week* article reviewing the **PTAC guidelines** is available at: http://blogs.edweek.org/edweek/DigitalEducation/2014/02/us_ed_dept_issues_guidance_on_.html

A *New York Times* article discussing the **federal PTAC guidelines** is available at: http://bits.blogs.nytimes.com/2014/02/25/regulators-weigh-in-on-online-educational-services/

The toolkit from the **Consortium for School Networking** can be viewed at: http://cosn.org/sites/default/files/Protecting%20Privacy%20in%20Connected%20Learning%20Toolkit%202014_0.pdf

Additional information on **FERPA** is available at: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

The Fordham Center on Law and Information Privacy published a report on **protecting student privacy** in the era of **cloud computing.** The report can be read at: http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip

Digital Learning Now has broad **guidelines for protecting student privacy** in personalized learning environments, available at: http://www.digitallearningnow.com/blog/trust-in-the-classroom-protecting-student-data-privacy-and-security/

The **Data Quality Campaign** has published several articles on considerations surrounding privacy, security, and confidentiality when **schools collect and use student data.** See: http://dataqualitycampaign.org/action-issues/privacy-security-confidentiality/

The Federal Trade Commission updated its **Children's Online Privacy Protection Act FAQs** to offer additional guidance about when schools can provide consent on behalf of parents to third-party providers. See: http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions#Disclosure