Establishing a Robust Student Data Privacy Culture

Action Ideas for School Districts

provided by:

catchon An ENA Affiliate

FORESIGHT LAW+POLICY

SETDA LEADERSHIP • TECHNOLOGY • INNOVATION • LEARNING

Introduction

New technologies offer educators powerful tools to collect, analyze, and use data to help prepare students for academic and workforce success. Effective education data analytics can reveal persistent achievement gaps, support improved instruction, and provide powerful evidence for making administrative and policy decisions. Armed with real data—their data—districts have a responsibility to produce data-driven insights for their students and teachers.

Moreover, school systems have an ethical and legal obligation to protect each student's privacy. Technology can help promote privacy by helping schools effectively encrypt sensitive data, monitor software downloads, and use and record data disclosures, but districts must also develop and adopt broader strategies to ensure that student data is secure and used only for legitimate educational purposes.

CatchOn is committed to promoting student data privacy by helping school districts cultivate a culture that values appropriate data use and embraces data privacy best practices. With that goal as our guide, this paper presents practical ideas district leaders may implement to make data privacy a prominent part of the fabric of classrooms, schools, and school districts. This paper also highlights key federal and state student data privacy expectations and requirements that educators and administrators should understand. Successful data use and privacy practices vary greatly within and among states, but we hope this guide will serve as a useful planning tool for any school district - big or small, rural or urban, privacy leader or novice - aspiring to foster a system-wide commitment to student privacy.

5 Action Ideas for Establishing a Student Data Privacy Culture

1. Develop a data use vision and strategy
2. Adopt and promote privacy principles
3. Offer innovative training and resources
4. Engage parents to earn trust
5. Ensure local privacy policies properly integrate federal and state requirements

ACTION IDEA ONE:
Develop An Informed Data Use Strategy

Developing a culture that effectively protects student data privacy requires educators and administrators to understand the district's expectations and strategies for using data in ways that support student achievement. If districts develop student data privacy policies without undertaking a systematic effort to understand the critical role data plays in supporting teaching and learning, then their policy practices may be crafted from isolated reviews of federal and state requirements, model privacy policy language designed for other contexts, or provide dated privacy materials that may fail to account for changes in law and regulation. All of these scenarios inadvertently make it harder for schools to use data to better serve students and families.

School districts can simultaneously protect and leverage student data by first establishing an inclusive and collaborative process for developing, adopting, and implementing a districtwide data strategy. To that end, the data use planning process should examine how the district manages data collection and its reporting obligations, which may issue from federal accountability requirements and the state's Department of Education requests for data concerning enrollment, demographic, finance, and safety.

The review process must also analyze elective data practices. This analysis should involve the data schools collect to support and improve instruction; the data the district uses to make operational decisions and improvements; and the data provided to parents to support student welfare. In each instance, the planning process should confirm that the data shared with stakeholders is accurate, understandable, and relevant to the purpose for which it was collected. Doing so will ensure that individual stakeholders value data use and privacy practices in ways that are woven into the district's everyday functions.

Developing a culture that effectively protects student data privacy requires educators and administrators to understand the district's expectations and strategies for using data in ways that support student achievement.

ACTION IDEA TWO:
Adopt And Promote Privacy Principles

After developing a data use strategy, school districts should work with staff, parents, and other stakeholders to adopt clear privacy principles. This effort should be paired with a plan to integrate these principles into the district's operations, everyday language, and staff culture.

The principles should offer a high-level articulation of the district's commitment to privacy in a way that guides the development of a more detailed privacy policy. The principles also confer three additional benefits:

1. By offering the district's community a simple articulation of best privacy practices, principles help promote compliance districtwide.
2. Clearly stated principles foster trust and understanding within the community about the district's data uses.
3. Defined principles provide a framework that informs resolutions to problems that arise and future decisions regarding data use.

Ensuring districtwide compliance with complex state and federal privacy requirements can be challenging because they do not always align or use the same terminology. For instance, the federal Family Educational Rights and Privacy Act uses "education records" while Virginia state law refers to "scholastic records."[1] The resulting uncertainty can lead to insecurity and mistrust among stakeholders and hinder effective communication with parents.

Fortunately, federal and state laws and many privacy policies often share underlying privacy values and principles: promoting transparency, honoring individual consent, and securing data. Because effective privacy principles are by definition concise, they are easier to integrate into a district's daily operations, including communications to stakeholders. In short, good privacy principles promote community trust.

After developing a data use strategy, school districts should work with staff, parents, and other stakeholders to adopt clear privacy principles.

2

ACTION IDEA THREE:
Offer Innovative Training And Resources

Creating a robust privacy culture across a school district requires an effective and ongoing strategy for training educators how to use and safeguard student data. School districts should commit to deliver engaging and ongoing data-use professional development that:

1. Introduces basic privacy requirements;
2. Is tailored to each person's role;
3. Is firmly grounded in the district's data vision, data use strategies, and data privacy principles.

Why? Student data collected, used, and maintained by schools is protected by multiple federal and state laws and regulations. Educators will be more likely to acquire a working understanding of these privacy laws and best practices if they learn about them through the lens of their daily professional responsibilities and expertise as educators.

Educators should also be familiar with broadly applicable privacy obligations and concepts, such as FERPA's prohibition on disclosing personally identifiable information without the consent of a parent or eligible student.[2]

Additionally, staff members will benefit from supplemental training that provides more detail on the privacy requirements specific to their work.

Creating a robust privacy culture across a school district requires an effective and ongoing strategy for training educators how to use and safeguard student data.

For example:

- **Superintendents and administrators**. Tasked with responding to outside research requests, these leaders may benefit from in-depth training about FERPA provisions applicable to studies and program audits and evaluations.[3]
- **Teachers**. As users of instructional tools and software, teachers may benefit from training on the Children's Online Privacy Protection Act's prohibitions on third party collection and use of data from students younger than age 13.[4]
- **District analytical professionals**. In order to prevent violations of FERPA's disclosure exceptions, staff responsible for producing a district's public accountability reports may benefit from understanding how to properly de-identify aggregate data when publishing accountability or other aggregate student data.

Developing tailored privacy training consistent with the district's data practices will help ensure the efficacy of professional development.

ACTION IDEA FOUR:
Engage Parents To Earn Their Trust

Because federal and state privacy laws require school districts to notify parents about their privacy practices, district leaders should meaningfully engage parents to gather their perspectives when developing data privacy policies. Doing so will not only help ensure districts comply with federal and state laws—FERPA and certain states require annual notice to parents about their privacy rights, including the right to access and correct inaccuracies in their student's record—it will foster the kind of community engagement essential to the success of any data privacy strategy.

Without community understanding and approval of student data use and privacy principles and practices, confusion and distrust can spread, so it is imperative that districts communicate with parents clearly. Effective communications are those that emphasize clarity over legal language and are guided by a clearly articulated vision for data use and privacy.

Fortunately, many parents support the ways schools use data and have trust in their commitment to privacy. To wit, a 2017 Data Quality Campaign survey showed that 94% of parents now support teachers using data to ensure students receive the support and enrichment they need.

Also, 88% of parents trust that their child's school is keeping their child's data private and secure.[5]

But this invaluable trust can of course be lost, so district leaders must continually engage parents to nurture their trust.

Therefore, in addition to including parents in the planning and implementation process, districts should keep them abreast of ongoing data use successes and challenges. For example, districts should make clear what kinds of data they collect, how that data supports education, and how the district keeps it secure. To ensure community buy-in, districts should regularly provide forums at which parents can voice their views and concerns, such as town hall discussions, focus groups, and informal surveys. Finally, to demonstrate that parents have been heard, districts should subsequently communicate how parental feedback informed changes to the district's privacy practices.

District leaders should meaningfully engage parents to gather their perspectives when developing data privacy policies.

4

ACTION IDEA FIVE:
Ensure Local Privacy Policies Integrate Federal And State Requirements

Cultivating an effective districtwide privacy culture and climate requires alignment with federal, state, and local requirements. However, solely focusing a district privacy strategy on a rigid, compliance mindset is not likely to succeed.

Many official resources exist to help districts maintain compliance, but we have included a data privacy FAQs resource in this document to further help readers navigate this part of their privacy journey. This resource addresses highlights from federal and state law, along with a few additional sources of recommended reading. This FAQ is only for initial reference. Districts should always consult with their local counsel before making data privacy decisions.

Engaging educators, building leaders, partners, and parents in planning will help to produce a well-rounded data vision for a district and lay a strong cultural foundation for subsequent conversations about the school district's privacy principles, policies, and practices. It may also prompt immediate privacy improvements within the district by ensuring the district only collects and uses appropriate and relevant data. Additionally, planning collectively promotes transparency and allows for the creation of a public inventory of the district's data practices.

The assumptions stakeholders form through the planning process about the district's commitment to privacy and student focused data use will have ongoing importance. They will inform how educators teach, how building and district leaders manage their teams, and how parents engage with schools.

Cultivating an effective districtwide privacy culture and climate requires alignment with federal, state, and local requirements.

5

Federal Student Data Law Overview

Family Educational Rights and Privacy Act (FERPA)

FERPA provides parents or eligible students the right to inspect and review the student's education records and to request corrections to errors in the record.* These are records "directly related to the student" and "maintained" by a school or district. The law also requires school or school districts to secure parent or eligible student consent prior to disclosing a student's personally identifiable information, except in certain circumstances, and annually notify parents and eligible students of their FERPA rights.[6]

NOTE: *Student data that is not personally identifiable may be disclosed without consent and for any purpose.*[2]

FERPA FAQs

1. Which entities must comply with FERPA?

SHORT ANSWER: Every public elementary and secondary school and school district is subject to the Family Educational Rights and Privacy Act (FERPA).

DEEPER DIVE: FERPA applies to "educational agencies and institutions" that receive any U.S. Department of Education funding, including grants, subgrants, contracts, and subcontracts.[7]

The regulations apply to school districts because they are "agencies" authorized to "direct and control public elementary or secondary...institutions" and the regulations also apply to individual schools because they are an "institution" that "provides educational services or instruction, or both, to students."[8]

2. When is consent required by FERPA to disclose personally identifiable student data?

SHORT ANSWER: Schools and school districts must secure parent or eligible student consent before disclosing a student's personally identifiable information (PII). However, FERPA does provide some limited exceptions to this general consent requirement so long as the student data disclosures satisfy specific conditions and limitations.

DEEPER DIVE: FERPA generally requires educational agencies or institutions to obtain a parent or eligible student's consent prior to disclosing PII contained in the student's education record.[9] The law and regulations, however, specify a number of disclosure exceptions when parent or eligible student consent is not required.[10] These exceptions include practical accommodations designed to facilitate research, operational uses, health and safety decisions, accreditation reviews, and more, so long as the student data disclosures satisfy specific conditions and limitations. Although there are a number of exceptions to the consent requirement, there are three common exceptions school leaders should learn about first: (1) the school official exception; (2) the directory information exception; and (3) the audit and evaluation of state or federal programs exception.

** An eligible student is a student who has reached 18 years of age or is attending an institution of postsecondary education.*

3. What is FERPA's school official exception and how may it be used?

SHORT ANSWER: The school official exception permits schools or school districts to disclose personally identifiable student data without consent to a third party that is providing an outsourced service that a school or district employee would otherwise provide. The third-party partner must satisfy certain criteria and the student data disclosed to the partner must always remain under the control of the school or district.

DEEPER DIVE: The school official exception[11] permits disclosure of PII without parent consent or eligible student consent if the school or school district determines that the entity the data is being shared with:

1. Meets the school's or district's criteria for being a school official
2. Has a "legitimate educational interest" in the PII[12]

School districts, using locally defined and published criteria, may designate an entity as a school official consistent with the following FERPA requirements. "A contractor, consultant, volunteer or other party to whom an agency or institution has outsourced institutional services or functions may be considered a school official" provided that the party:

- "Performs an institutional service or function for which the agency or institution would otherwise use employees;
- Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and
- Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records".[13]

"Schools that designate an entity as a school official for this limited purpose must always have direct control of the data and must work with the partner entity to establish reasonable methods to ensure that [the entity] obtain[s] access to only those education records in which they have legitimate educational interests."[14] Additionally, the entity must adhere to FERPA's §99.33(a) redisclosure requirements by ensuring the information is used only for the purposes for which it was disclosed and that additional disclosures will only be made at the school or school district's direction and consistent with FERPA's disclosure limitations.

Although FERPA does not require a written agreement between the school and the third-party partner when using the school official exception, using a contract is an accepted best practice to ensure students' privacy is strictly protected and to ensure the data is only used consistent with the purpose for which it was disclosed.

FERPA FAQs, continued

4. Does FERPA permit sharing student data for research?

SHORT ANSWER: Yes. Two FERPA consent exceptions – the "audit or evaluation of state or federal programs exception" and the "studies exception" - permit schools or school districts to disclose personally identifiable student data for research, so long as certain conditions are satisfied.

DEEPER DIVE: Schools and school districts may disclose student PII required for research by using FERPA's audit or evaluation of federal or state education programs exception. FERPA's regulations permit "authorized representatives," such as researchers of state and local educational authorities to use student's education records in connection with an audit or evaluation of federal or state supported education programs.[15]

For example, schools and school districts are local educational authorities. FERPA does not define "state or local educational authority" but the Department of Education has said that the term includes school districts and other entities that "direct and control public elementary or secondary…institutions."[16]

State and federal supported "education program" means "any program that is principally engaged in the provision of education, including, but not limited to, … elementary and secondary education … and any program that is administered by an educational agency or institution."[17]

The regulations broadly define audit and evaluation. The Department of Education has broadly interpreted "evaluation" to "include all manner of studies, assessments, measurements, appraisals, research, and other efforts, including analyses of statistical or numerical data derived from education records."[18]

In order to use the audit and evaluation exception as a basis for sharing PII, a school district must designate partner researchers - as their "authorized representative." Participating partners must also ensure that the information provided to a researcher is only used to carry out the evaluation and must ensure that the research partner protects the PII from further disclosures or other uses (except as authorized), and destroys the PII as required by the regulations. Each of these requirements must be addressed in a written agreement.[19]

In addition to the "audit or evaluation" exception, FERPA also permits disclosures, without consent, of students' PII for "studies" to: (1) develop, validate, or administer predictive tests; (2) administer student aid programs; or (3) improve instruction.[20] This more narrowly focused research exception is useful in these specific circumstances. Similar to the audit or evaluation exception, the parties must enter into a written agreement that describes the terms of the data disclosure and use.

5. What is FERPA's directory information exception?

SHORT ANSWER: "Directory information" is information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Each school, unless there is an overarching school district directory information policy, decides what information specifically qualifies as "directory information" but they must provide notice of the definition to their current students and provide them a reasonable opportunity to opt-out of disclosing their information. Properly designated directory information may be disclosed, and redisclosed by third parties, for any purpose.

DEEPER DIVE: Schools or school districts may elect to disclose PII that is properly designated as "directory information," without securing parent or eligible student consent.[21] FERPA's regulations define "directory information" as "information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed."[22] The federal regulations and statute provide directory information examples, including the following student information, such as name, address, telephone listing, e-mail address, data of birth and more.[23] Directory information may not include a student's social security, disability status, free and reduced lunch status, or other information that if released would be harmful or considered an invasion of property.[24]

Directory information is only properly designated as such if a school or school district provides public notice to their students' parents of: (1) the types of personally identifiable information that the school or school district has designated as directory information; (2) the parent's right to opt-out of all or part of the directory information designation; and (3) the reasonable period of time within which they must object to the designation in writing.[25] A school or school district may disclose directory information of former students without complying with these notices and opt-out requirements but must honor past opt-out requests.[26]

Children's Online Privacy Protection Act

Schools should also become familiar with the Children's Online Privacy Protection Act (COPPA), which places limitations on a for profit entity's collection and use of data from children less than age 13. Although COPPA does not apply directly to schools or school districts, the law does apply to for profit companies, including app providers, that work with schools. Schools should ensure that their for-profit partners are meeting COPPA's requirements and that teachers are not using applications that collect the data of students less than age 13, without their school's knowledge.

COPPA, enforced by the Federal Trade Commission, "applies to operators of commercial websites and online services directed to children under the age of 13 that collect personal information."[27] In addition, "it applies to operators of sites and online services geared toward general audiences when they have 'actual knowledge' they are collecting information from children under 13 ... [and] to operators when they have 'actual knowledge' they are collecting personal information from users of another site or online service directed to kids under 13."[28] Websites and online services covered by COPPA must post privacy policies, provide parents with direct notice of their information practices, and get verifiable consent from a parent or guardian before collecting personal information from children.[29]

CatchOn's Commitment to Promoting Student Data Privacy

CatchOn proudly supports and has signed the Student Privacy Pledge. As a software as a service solution that is both a software discovery and usage tracking tool for applications, CatchOn is committed to protecting student data. Our 360-degree approach to student data privacy helps you keep your data safe and provides you real-time visibility into the learning tools being used in your school district.

How Does CatchOn Help Your School District Stay Compliant?

The CatchOn platform supports privacy compliance at both federal and state levels by:

- Giving users the ability to mark and categorize their applications as approved or not approved by the district. Users can sort, download, and export a list of approved or unapproved applications to share with district personnel, stakeholders, and parents
- Enabling education leaders to see the software applications being used on their school devices, both inside and outside the classroom, meaning administrators can quickly diagnose applications vulnerable to student data privacy policies
- Empowering districts with the ability to publish shareable lists of district approved applications and correlating agreements that display the specific student data being collected by each app

See how CatchOn specifically helps districts stay compliant with education privacy laws below.

Education Law What is Required at a Glance	**CatchOn's Solution** How CatchOn Can Help You Stay Compliant	
Review 3rd party agreements	Affords quick access to 3rd party websites and privacy policies	✓
Ensure district privacy/security policies are aligned	Provides ability to mark and categorize applications as approved or not approved by the district	✓
District data protection office	Enables education leaders to see software applications used on school devices, both inside and outside the classroom; Empowers leaders to diagnose applications vulnerable to student data privacy policies	✓
Continuous review for compliance	Provides the ability to monitor known and unknown apps for compliance	✓
Parental notifications	Enables districts to post and share approved and monitored apps with parents using automated reports	✓
Breach notification plan	Provides the ability to gather data on EdTech usage, applications privacy policies, and district purchases to avoid vulnerabilities	✓
Align to NIST framework and FERPA policies	Tracks only de-identified aggregated information, and PII stays on the district's server; CatchOn has signed the student data privacy pledge	✓
Privacy training	Enables districts to facilitate training opportunities by leveraging data analytics that track data usage, trends, and impact	✓

Experience the Difference at www.catchon.com

Wise Investments

Boost Efficiency. Identify which apps teachers are actually using to better allocate resources

Early KPIs. Measure the performance of new investments as soon as you make them

Trend Detection

Eliminate Gaps in Data. Receive detailed reports on data at the district, school, and class level

Champion Network. Get performance data from our client schools to learn the latest improvements to EdTech

Subscription Management

Waste-Free Tech. Get real-time, class-level data to know how many subscriptions and licenses are truly needed

Streamlined Renewal. Know when renewals are due to prevent gaps in service

Improved Training

Professional Development. Identify and disseminate the latest best practices

Confirmed Deployment. Ensure instructors are incorporating effective EdTech

Student Data Protection

Peace of Mind. Rest worry-free knowing CatchOn can only access de-identified aggregated data

Rigorous Review. Monitor the behavior of all apps to ensure student privacy is maintained

Effective Usage

Address equity gaps. Discover how students use their apps and devices, both inside and outside of class

Save Money. Find effective free alternatives to costly apps

Custom Visibility

Loud and Clear Reporting. Customize the dashboard and reporting system to achieve your unique goals

Data Clarity. Bring your data to life with clear, detailed analysis to drive effective strategies

Student Achievement

Immediate Reporting. Get up-to-the-minute results to keep students from falling behind

Student-Centered Analytics. Evaluate your tech based on how it effects real students

Learn how CatchOn aligns to your state education privacy laws.

Select state reviews are available at www.catchon.com/privacy-laws/

An ENA Affiliate
catchon®

Recommended Reading Appendices

Action Idea One Recommended Reading:

- The Art of the Possible: Data Governance Lessons Learned from Kentucky, Maryland, and Washington, Data Quality Campaign
- Transparency Best Practices for Schools and Districts - September 2014, U.S. Department of Education Privacy and Technical Assistance Center (2014)
- Using Evidence to Strengthen Education Investments, U.S. Department of Education
- How Data Can Support Student Success from Early Learning to Workforce, Data Quality Campaign
- Using Student Achievement Data to Support Instructional Decision Making, IES What Works Clearinghouse

Action Idea Two Recommended Reading:

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Fair Information Practices, Center for Democracy and Technology
- Trusted Learning Environment Practices, Consortium for School Networking

Action Idea Three Recommended Reading:

- How Data Can Support Student Success from Early Learning to Workforce, Data Quality Campaign
- Using Student Achievement Data to Support Instructional Decision Making, IES What Works Clearinghouse
- Protect Your Students' Privacy, Common Sense Education

Action Idea Four Recommended Reading:

- What Parents Need to Know about their Student's Data, U.S. Department of Education Privacy and Technical Assistance Center
- A Parent's Guide to Student Privacy, Center for Democracy and Technology
- How Data Empowers Parents, Data Quality Campaign

Action Idea Five Recommended Reading:

- Trusted Learning Environment Seal Program, Consortium for School Networking
- Integrated Data Systems and Student Privacy, U.S. Department of Education Privacy and Technical Assistance Center
- Complying with COPPA, U.S. Federal Trade Commission

Endnotes

[1] 20 U.S.C. 1232g(a)(4); Code of Virginia, § 22.1-289 Transfer and management of scholastic records

[2] 20 U.S.C. § 1232g(b)(1)

[3] 20 U.S.C. § 1232g(b)(1)(C) and (F)

[4] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505

[5] Poll Shows Parents Value, Trust, and Rely on Education Data, Data Quality Campaign, Available online at http://bit.ly/37PSAac

[6] 20 U.S.C. § 1232g; 34 C.F.R. 99.1

[7] Ibid.

[8] 34 C.F.R. § 99.1(a)

[9] 20 U.S.C. § 1232g(b) and (d); 34 CFR § 99.30-99.39

[10] 20 U.S.C. § 1232g(b); 34 C.F.R. § 99.31

[11] 34 C.F.R. § 99.31(a)(1)

[12] 20 U.S.C § 1232g(b)(1)(A); 34 C.F.R. § 99.31(a)

[13] 34 C.F.R. § 99.31(a)(1)(i)(B)

[14] 34 C.F.R. § 99.31(a)(1)(ii)

[15] 34 C.F.R. § 99.35(a)(1) and (a)(3)

[16] Department of Education, 34 C.F.R. Part 99, Family Educational Rights and Privacy Act, Final Rule, p. 75607 (December 2011)

[17] 34 C.F.R. § 99.3

[18] Department of Education, 34 C.F.R. Part 99, Family Educational Rights and Privacy, Proposed Rule, p.15586 (March 24, 2008)

[19] 34 C.F.R. § 99.35; See also 20 U.S.C. § 1232g(b)(3)

[20] 20 U.S.C. § 1232g(b)(1)(F)

[21] 20 U.S.C. § 1232g(b)(2); 34 C.F.R. § 99.31(a)(11)

[22] 34 C.F.R. § 99.3

[23] 34 C.F.R. § 99.31; See also 20 § U.S.C. 1232g(a)(5)(A)

[24] Ibid.

[25] 34 C.F.R. § 99.37(a)

[26] 34 C.F.R. § 99.37(b)

[27] 15 U.S.C. § 6501 et. seq., Children's Online Privacy Protection Act of 1998;
Federal Trade Commission, Children's Online Privacy Protection Rule: Not Just for Kids' Sites,
https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites

[28] Federal Trade Commission, Children's Online Privacy Protection Rule: Not Just for Kids' Sites,
https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites

[29] Children's Online Privacy Protection Rule, FAQ,
https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites

Acknowledgments

SETDA

LEADERSHIP • TECHNOLOGY • INNOVATION • LEARNING

Founded in 2001, the **State Educational Technology Directors Association (SETDA)** is the principal nonprofit membership association representing US state and territorial educational technology leaders. Our mission is to build and increase the capacity of state and national leaders to improve education through technology policy and practice. For more information, please visit setda.org.

FORESIGHT LAW+POLICY

Foresight Law + Policy is a national education law firm based in Washington, D.C. Our lawyers and other professionals counsel education leaders, nonprofit organizations and companies working to strengthen public education and prepare all kids for success. For more information, please visit www.flpadvisors.com.
Contributing Author: Reg Leichty, Founding Partner

An ENA Affiliate

catchon®

CatchOn is an expansive data analytics tool that compiles real-time data on every device, enabling school districts to make data-informed decisions about the apps and online tools their educators and students are using. In 2018, CatchOn joined forces with ENA, a leading provider of comprehensive technology solutions to education institutions and libraries across the nation. Collectively, CatchOn and ENA leverage their respective resources and expertise to deliver critical services and solutions that help school districts produce positive outcomes in the communities they serve. For more information, please visit www.catchon.com, call **866-615-1101**, or email **solutions@catchon.com**