ENDNOTES

i Archived: A Nation At Risk. Accessed February 18 2013. https://www2.ed.gov/pubs/NatAtRisk/risk.html

ii Lai and Schildkamp (2013), Dunn and Ariola (2011) and Faria, Heppen, et al. (2012); Data Literacy Brief. Accessed February 18 2013. http://www.dataqualitycampaign.org/files/DQC-Data%20Literacy%20Brief.pdf

iii Blanc and Bulkley, et al. (2010). Learning to Learn From Data: Benchmarks and Instructional Communities. Peabody Journal of Education. Volume 85: pgs. 205–225, 2010.

iv US Dept. of Education. Legislative History of Major FERPA Provisions. Accessed March 24, 2014. http://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html

v Tennessee Code Annotated 10-7-504; Tennessee Code Annotated 49-2-211.

vi Data Quality Campaign Infographic. Accessed March 24, 2014. http://www.dataqualitycampaign.org/files/Data-Rich%20Year%20Infographic.pdf

vii Data Literacy Brief. Accessed March 24, 2014. http://www.dataqualitycampaign.org/files/DQC-Data%20Literacy%20Brief.pdf

viii Lai and Schildkamp (2013) and Faria, Heppen, et al. (2012); Data Literacy Brief. Accessed February 18 2013. http://www.dataqualitycampaign.org/files/DQC-Data%20Literacy%20Brief.pdf

Kerr and Marsh, et al. (2006). Strategies to Promote Data Use for Instructional Improvement: Actions, Outcomes, and Lessons from Three Urban Districts.

ix Blanc and Bulkley, et al. (2010). Learning to Learn From Data: Benchmarks and Instructional Communities. Peabody Journal of Education. Volume 85: pgs. 205–225, 2010.

x Carlson, Borman and Robinson (2011). A Multistate District-Level Cluster Randomized Trial of the Impact of Data-Driven Reform on Reading and Mathematics Achievement.

Dunn and Ariola (2011); Data Literacy Brief. Acessed February 18 2013. http://www.dataqualitycampaign.org/files/DQC-Data%20Literacy%20Brief.pdf

xi OECD. Strong Performers and Successful Reformers in Education Lessons from PISA 2012 for the United States. Accessed April 15, 2014. http://www.oecd.org/pisa/keyfindings/PISA2012_US%20report_ebook(eng).pdf

xii Means, Padilla, Gallager (2010). US Dept. of Education. Use of Education Data at the Local Level From Accountability to Instructional Improvement.

xiii Data Quality Campaign Infographic. Accessed February 4, 2014. http://www.dataqualitycampaign.org/files/Data-Rich%20Year%20Infographic.pdf

xiv Give Parents Access to Useful Data. Strategy 2.2: Empower parents with clear and useful data. Accessed February 12, 2014. http://www.studentsfirst.org/policy-agenda/entry/clear-and-useful-school-data

xv Information courtesy of the following sources: Data Quality Campaign. "From Compliance to Service." Accessed February 19, 2014. http://www.dataqualitycampaign.org/files/1455_From%20Compliance%20to%20Service.pdf, SAS EVAAS. Misconceptions about Value-Added Reporting in Tennessee. Retrieved April 3, 2014 from http://www.tn.gov/education/doc/TN%20Misconceptions_About_TVAAS.pdf.,

National Center for Education Statistics. "About Us." Accessed April 10, 2014. http://nces.ed.gov/about/

US Dept. of Education. "Education Dashboard." Accessed April 10, 2014. http://dashboard.ed.gov/dashboard.aspx; http://dashboard.ed.gov/about.aspx

xvi US Dept. of Education. "Higher Education Opportunity Act." Accessed April 10, 2014. See Section 113: http://www2.ed.gov/policy/highered/leg/hea08/index.html

US Dept. of Education. "No Child Left Behind." Accessed April 10, 2014. See Section 9531: http://www2.ed.gov/nclb/landing.jhtml?src=pb

Government Printing Office. "Education Sciences Reform." Accessed April 10, 2014. See Section 182: http://www.gpo.gov/fdsys/pkg/PLAW-107publ279/pdf/PLAW-107publ279.pdf

Government Printing Office. "Title I Amendments to the Individuals with Disabilities Act." Accessed April 10, 2014. See Section 616: http://www.gpo.gov/fdsys/pkg/BILLS-108hr1350enr/pdf/BILLS-108hr1350enr.pdf

xvii The Tennessean. "TN Ed commissioner to feds: Student data won't be shared." Accessed April 10, 2014. http://www.wbir.com/story/news/local/education/2014/01/24/tn-ed-commissioner-to-feds-student-data-wont-be-shared/4855183/

xviii US Dept. of Education. Legislative History of Major FERPA Provisions. Accessed March 24, 2014. http://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html

xix US Dept. of Education. "Protecting Student Privacy While Using Online Educational Services. Accessed February 25, 2014. http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services

xx Tennessee Code Annotated 10-7-504; Tennessee Code Annotated 49-2-211.

xxi TN Dept. of Education. "Research: Data Requests." Accessed March 24, 2014. http://www.state.tn.us/education/research/datarequests_000.shtml

US Dept. of Education—Privacy Technical Assistance Center. "PTAC Handout."Accessed April 23, 2014. http://ptac.ed.gov/sites/default/files/FERPA%20Exceptions_HANDOUT_horizontal.pdf

xxii Tennessee Code Annotated 49-2-211

xxiii Metro Nashville Public Schools: "Conducting Research within MNPS" Page. Accessed February 17, 2014. http://www.mnps.org/Page66332.aspx.

xxiv US Dept. of Education. "Protecting Student Privacy While Using Online Educational Services. Accessed February 25, 2014. http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services

US Dept. of Education—Privacy Technical Assistance Center. "PTAC Handout."Accessed April 23, 2014. http://ptac.ed.gov/sites/default/files/FERPA%20Exceptions_HANDOUT_horizontal.pdf

xxv Fordham CLIP. "Privacy and Cloud Computing: Cloud Storage Use in School Systems." December 2013. http://instructionaltechtalk.com/cloud-storage-use-in-school-systems/.

xxvi Fordham CLIP. "Privacy and Cloud Computing." December 2013.http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip

xxvii Fordham CLIP. "Privacy and Cloud Computing: Cloud Storage Use in School Systems." December 2013. http://instructionaltechtalk.com/cloud-storage-use-in-school-systems/.

xxviii US Dept. of Education. "Myths and Facts about Standards and Federal Policy." Accessed March 24, 2014. http://www.ed.gov/k-12reforms/standards

xxix US Dept. of Education—Privacy Technical Assistance Center. "PTAC Handout."Accessed April 23, 2014. http://ptac.ed.gov/sites/default/files/FERPA%20Exceptions_HANDOUT_horizontal.pdf

xxx US Dept. of Education. "Protecting Student Privacy While Using Online Educational Services. Accessed February 25, 2014. http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services.

xxxi Metro Nashville Public Schools: "Conducting Research within MNPS" Page. Accessed February 17, 2014.http://www.mnps.org/Page66332.aspx.

xxxii Data Quality Campaign. "Oklahoma Gets Guidelines, Protections." Accessed February 17, 2014.

http://dataqualitycampaign.org/blog/2013/09/oklahomas-new-student-data-act-sets-guidelines-protections.

xxxiii Data Quality Campaign. "Oklahoma's New Student DATA Act Sets Guidelines, Protections." Accessed April 16, 2014. http://dataqualitycampaign.org/blog/2013/09/oklahomas-new-student-data-act-sets-guidelines-protections/

xxxiv Idaho Senate Bill No. 1296. Accessed April 15, 2014. http://www.legislature.idaho.gov/legislation/2014/S1296.pdf

xxxv Tennessee General Assembly. "Summary: House Bill 1549/Senate Bill 1835." Accessed April 25, 2014. http://wapp.capitol.tn.gov/apps/billinfo/BillSummaryArchive.aspx?BillNumber=HB1549&ga=108.

xxxvi Tennessee General Assembly. "Summary: House Bill 1549/Senate Bill 1835." Accessed April 25, 2014. http://wapp.capitol.tn.gov/apps/billinfo/BillSummaryArchive.aspx?BillNumber=HB1549&ga=108.

xxxvii Education Counsel LLC. "Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policymakers." Accessed April 16, 2014. http://www.educationcounsel.com/docudepot/articles/EducationCounsel%20Guidance%20on%20State%20Student%20Privacy%20and%20Security%20Policies%20-%204838-6763-1641%20v%201.pdf

xxxviii PTAC. "FERPA Exceptions." Accessed April 25, 2014. http://ptac.ed.gov/sites/default/files/FERPA%20Exceptions_HANDOUT_portrait.pdf

xxxix Idaho Senate Bill No. 1296. Accessed April 15, 2014. http://www.legislature.idaho.gov/legislation/2014/S1296.pdf

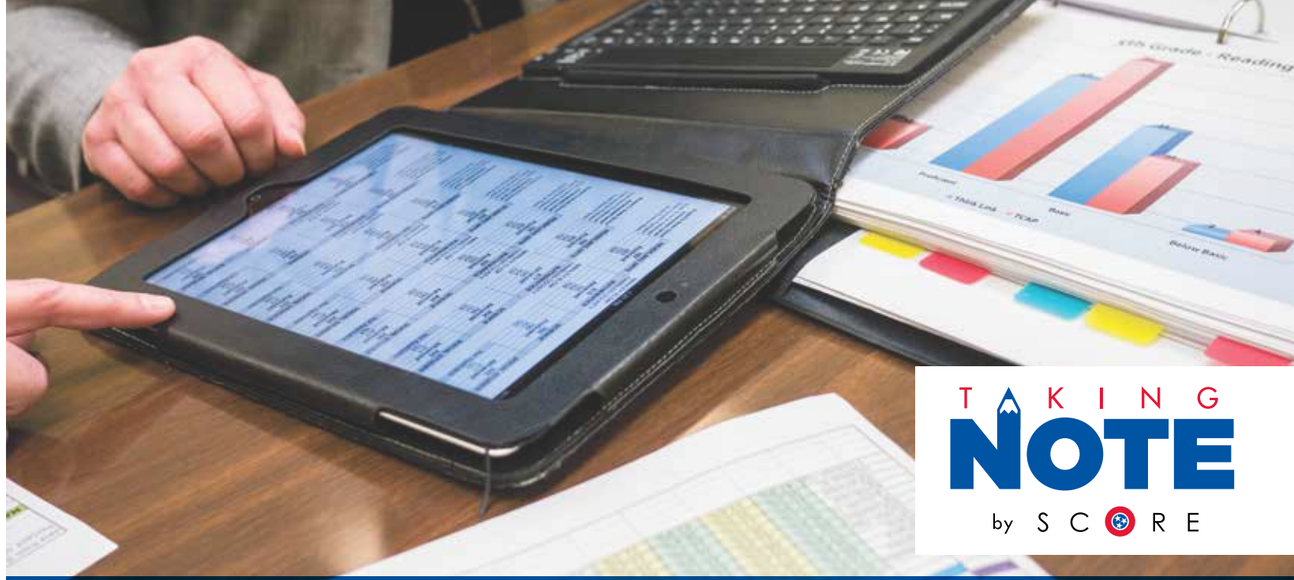
xl ALEC. "Model Legislation." Accessed March 24, 2014. http://www.alec.org/model-legislation/student-data-accessibility-transparency-accountability-act/.

US Dept. of Education. "Protecting Student Privacy While Using Online Educational Services. Accessed February 25, 2014. http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services.

xli Houston Independent School District. Software Ratings for Parents. Accessed April 15, 2014. http://www.houstonisd.org/Page/109830

xlii Consortium for School Networking. "Protecting Privacy in Connected Learning Toolkit." March 1, 2014. https://www.documentcloud.org/documents/1104427-cosnprivacytoolkit.html

TAKING NOTE by SCORE



UNDERSTANDING STUDENT DATA PRACTICES: USAGE AND PRIVACY

JUNE 2014

EXECUTIVE SUMMARY

Since the early 1980s with the release of reports such as *A Nation at Risk*, Americans have been using data to define and measure student achievement.[i] Education data is any type of information (like student attendance, demographics, or success in college and the workforce) that helps parents, educators, and policymakers make informed decisions about education. Research indicates that using data can lead to an increase in student performance and a decrease in achievement gaps.[ii] This happens when schools use data to set up student interventions and teachers use data to inform instruction.[iii] To enable this, student data must be stored properly and used appropriately.

As technology and education reforms have expanded, concerns regarding data security and usage have been voiced by some parents and policymakers. This memo explores issues related to data use and privacy, with a specific focus on the Tennessee context, to explain current policies and recent legislation and offer recommendations for addressing concerns about data use and privacy. The memo provides recommendations to ensure that Tennessee utilizes data in a smart way while protecting student privacy.

For decades, protections of student privacy have been built into state and federal law. The Family Educational Rights and Privacy Act (FERPA) created a framework to safeguard student privacy, and the state policies that followed throughout the years complement these protections.[iv] For example, Tennessee law protects student privacy rights in accordance with FERPA law and regulation, including the confidentiality of educational records and protection of student identity.[v]

Tennessee's commitment to smart data usage, while maintaining student privacy, should be reflected in the state's policies on student data privacy. Key components of a balanced state policy include: increased transparency and review of information collected, increased local district training and capacity-building, and employment of a Chief Privacy Officer to guide the state and local districts in ensuring student protections. Also, state policy should support educators' ability to use data to improve instruction. This includes avoiding policy, through regulation or statute, which prevents useful

SCORE 1207 18th Avenue South, Suite 326, Nashville, TN 37212 — tel 615.727.1545 — fax 615.727.1569 — **www.tnscore.org**

data practices from happening and any measure that limits the effective use of data for educational purposes.

With this in mind, it is important that the right data are collected for the right reasons and used for the right purpose. Tennessee has the opportunity to both protect student privacy and promote appropriate practices that allow data to be used to dramatically improve the educational experience of all students.

WHY USE DATA

Data are used in Tennessee's classrooms on a daily basis by teachers to help shape instruction, by families to monitor their students' progress, and by schools to meet their improvement goals.[vi] As Tennessee continues to strive for higher student achievement, effective use of student data is integral to success. [vii]

Research reiterates the importance of using data for student improvement. The findings of several studies show that student achievement improves when teachers receive training and when schools utilize the data available to make decisions.[viii] Strong evidence reveals that the strategic use of assessments contributes to instructional improvement.[ix] These results also suggest that districts and schools can use data to help close achievement gaps and that the use of data-driven changes can lead to significant districtwide improvements in student math and reading achievement.[x] In fact, using data to help students succeed is a priority in school systems nationwide, as global competition requires a highly educated workforce with high achievement in math and reading. [xi] For these reasons, data systems are expected to play an important role in improving educational decision-making at all levels.[xii]

WHAT ARE SOME WAYS THAT TEACHERS USE DATA?

Teachers constantly use data to make decisions about their instruction. Here are examples of how a teacher might use data throughout the year.

SUMMER

A teacher receives his or her students' data from the previous year and uses this data to determine what students already know, form guided reading groups that target growth for students based on their previous performance, and plan strategic lessons for the year.

FALL

The teacher gives a quick quiz at the end of each lesson to see if students understand the content.[xiii] Reflecting on the quick quiz, the teacher determines where any confusion may be, thinks creatively about why a misunderstanding may have occurred, and re-teaches the topic for individual or small groups of students as needed to clarify the learning and ensure students are prepared for the next lesson.

THROUGHOUT THE SCHOOL YEAR

- **Benchmark assessments** are given to assess mastery of academic standards for individual students.
- **Customized reports for families** are distributed during parent conferences. The teacher uses data, which indicate how the child grew academically compared to the school, district, and state averages, to direct the conference.[xiv]
- **Intervention groups** are also formed from assessment results. The teacher is especially conscious of where each student is struggling and makes sure all students receive targeted attention to master each topic.

SPRING

The teacher continues to use assessments in the classroom, and the results are used to inform parent reports, intervention groups, and targeted lessons. In April, students take the Tennessee Comprehensive Assessment Program (TCAP) to show mastery.

SUMMER

Results from the TCAP assessments are distributed, and teachers, parents, and schools can see how much students improved academically throughout the year. Once again, teachers use these results to plan for the students they will receive next year.

WHAT TYPES OF DATA INFORM DECISION-MAKING?

Because teachers and schools use student information to increase student achievement, analysis of the data is used to determine where students and schools are on the path to learning growth. Below are some examples of the types of information that inform decision-making at the local, state, and federal level.[xv]

LOCAL SCHOOLS

Daily Classroom Assessments: Teachers use quizzes and independent work, in addition to tests, to ensure each student is on track to be successful. Then this information is used to adjust instruction.

Attendance and Academic Information: Schools record students' absences and transfers to comply with compulsory attendance laws, and teachers often input grades into an online gradebook. Parents and students can access this information to monitor progress.

DISTRICTS

Special Populations: District officials provide support and progress monitoring for schools with students in special populations, like Special Education and English Language Learners.

Formative Assessments: Districts contract with specialists to create or purchase off-the-shelf assessments to view schools' literacy and subject-area growth.

STATE: TN DEPT. OF ED. (TDOE)

Note: All data reported to the TDOE are assigned a Unique Student Identifier (not a Social Security Number), which contains "coded" student information.

State Longitudinal Data System: This system combines state and local resources to show student growth over time, which allows educators to provide meaningful learning for individual students. The TDOE supports all districts and schools by providing analysis. This information is also used to answer broader questions asked by policymakers.

Tennessee Value Added Assessment System (TVAAS): TVAAS uses data from Tennessee's achievement tests (TCAP) to calculate yearly growth for all students in the state. TVAAS compares a student's growth in the current school year to a student's average growth in previous years, ensuring that a student's background will not affect the accuracy of the measure.

FEDERAL: US DEPT. OF ED. (USDOE)

National Center for Education Statistics: The data collected from states are reported to the U.S. Department of Education (USDOE) in aggregated form (absent of personally identifiable student information). The data are analyzed and available for important research on many education topics. Many leaders at the federal level, like Congress, educational organizations, business leaders, and the general public rely on the use of this data to see how the nation is doing and to plan for the future.

Education Dashboard: The USDOE provides this public tool for the nation to monitor this overall goal: the highest college graduation rate in the world. The dashboard shows how each state is progressing.

SCORE 1207 18th Avenue South, Suite 326, Nashville, TN 37212 — tel 615.727.1545 — fax 615.727.1569 — **www.tnscore.org**

DATA USAGE AND PRIVACY: *Federal, State, and Local Policies*

As public debate about data privacy and use continues, some concerns have been raised about the ways the federal government, states, and local districts use student data. Since there is overlap between federal, state, and local laws and policies, data usage and privacy are best addressed in a comprehensive examination. Common concerns surround three main areas of data usage and privacy: **collection, access,** and **storage**. For example, the following common questions stem from these three concerns: Is there a national student database? Who has access to student data? How do schools and government agencies store data?

Responsibility lies at the federal, state, and local levels to encourage appropriate data use and ensure student privacy. The graphic below is a comprehensive examination of the policies that are in place to address these common concerns and includes recommendations to enhance student data privacy.

	LEGAL PROTECTIONS	RECOMMENDATIONS *(detailed on pages 9-11)*
DATA COLLECTION	**Why does the government collect data? Is there a national student database?** Data are used at the federal level to monitor states' improvement and compare student outcomes nationally. States collect data to comply with federal laws and hold their school districts accountable. Federal and state laws exist to protect the amount of data collected and its usage for improving student achievement. **Federal** **The US Department of Education (USDOE) is prohibited from creating a national database of personally identifiable student information by these laws[xvi]:** • Higher Education Act of 2008 • No Child Left Behind • Education Sciences Reform Act • Individuals with Disabilities Education Act **State** **States only report aggregate information from districts (without personally identifiable student information) to show school and district achievement.** • In January 2014, Tennessee Commissioner of Education Kevin Huffman stated, along with 33 other state commissioners, in a letter to US Education Secretary Duncan that "states would not release personally identifiable student information to the US Department of Education or any other federal agency."[xvii]	***Continue data collection.*** *Tennessee's schools and districts use data to adjust instruction, and educators and parents use data to monitor student progress.* ***Inventory and fine tune.*** *When the data collection is not necessary, state officials should be allowed to revise collection and reporting.* ***Inform the public.*** *Parents and community members should have information about what data are collected about students and how this data informs individualized instruction.*

	LEGAL PROTECTIONS	RECOMMENDATIONS *(detailed on pages 9-11)*
DATA ACCESS	**Who has access to student data? Is student data used for research or marketing?** Federal and state education officials can access protected student data to monitor state and district progress. Also, researchers can seek approval to access relevant student information that must be protected under federal and state laws, and district policies. **Federal** **The Family Educational Rights and Privacy Act (FERPA) limits access to three groups of people: students, parents, and school officials.** Parental rights include the ability to inspect, amend, and control the disclosure of personally identifiable student information. Parents can also issue complaints to investigate whether violations have occurred.[xviii] Sometimes schools and districts contract with third-party organizations to provide online services. In these situations, organizations are given similar access to student data as school officials and are held responsible for protecting student privacy under FERPA agreements. These agreements require the same protections of personally identifiable information including consequences for violating the contract. Additionally, these federal laws address marketing:[xix] • **Protection of Pupil Rights Amendment (PPRA)**—prohibits student information from being used for marketing purposes and gives rights to parents to inspect and opt out of any non-educational surveys. • **Children's Online Privacy Protection Act (COPPA)**—requires websites and online services to gather "verifiable parental consent" before collecting and using information provided by children under 13. **State** **FERPA is authorized as spending clause legislation, and states are required to comply with its protections to receive federal funding.** Tennessee has two major provisions in annotated code that outline these protections:[xx] • **T.C.A. 10-7-504—** is more restrictive than FERPA and requires confidentiality of student records and the appropriate use of information that is not personally identifiable. • **T.C.A. 49-2-211—**requires every district to develop policies outlining the rights of parents and students and guidelines for educators in administering surveys or evaluations of students. **The Tennessee Department of Education (TDOE) permits education researchers to access data beyond what is publicly available if they meet several FERPA standards.** The TDOE screens applicants to ensure they have security systems in place and align their work with research priorities set by the department. The researchers must sign an agreement to comply with these standards.[xxi]	***Create a Chief Privacy Officer (CPO).*** *The CPO within the TDOE should oversee the implementation of all student privacy policies.* *The CPO should also aid districts with training of their employees and provide a model for their own data privacy policies in the following areas:* • *Transparency* • *Awareness of legal provisions* • *Inventory of all online services* • *Control of service agreements* ***The USDOE recently created a CPO position (along with its Privacy and Technical Assistance Center) to assist states in establishing sound privacy policies and ensure federal privacy protections. Additional information can be found here: http://ptac.ed.gov/***

	LEGAL PROTECTIONS	RECOMMENDATIONS *(detailed on pages 9-11)*
DATA ACCESS (CONT.)	**Local Districts** **Tennessee law requires local school districts to adopt policy regarding surveys and research.**[xxii] Some districts have clear research and data related policies. For example, Metropolitan Nashville Public Schools (MNPS) has a detailed webpage on this topic that mirrors the state's approval policy.[xxiii] (See Timely Topics example.)	
DATA STORAGE	**How do schools and government agencies store data? What is "cloud storage" and what protections exist for its use?** Just as the Internet provides the ability to access email from any computer, a cloud storage system can be used for password-protected access to data within student management systems from multiple sites. In fact, 95% of districts use cloud services for housing student performance data and daily operations information.[xxvi] Federal and state protections guide the usage of cloud storage.	***Include storage safeguards within state policies.*** *For example, states can:* *1) Limit use for educational, non-commercial uses.* *2) Impose civil penalties for improper use from third-parties.* *3) Assign a Chief Privacy Officer who ensures that districts and staff are trained to handle confidential information.* *4) Give cloud-use guidance to district through the Chief Privacy Officer or another official.*
	Federal **FERPA provides specific guidance to states and districts for cloud usage.**[xxvii] Ultimately, each school and district is still the owner of the information stored in the cloud system they choose to use, not any federal agency or third party.	
	State **Tennessee is required to ensure security of cloud and all other storage systems.** Under FERPA regulations, states and districts must follow guidelines (see recommendations) from the USDOE that protect student privacy.[xxviii]	

TIMELY TOPICS IN DATA USE: LOCAL AND STATE EXAMPLES

The following examples show how current district and school policies apply federal and state protections of student data privacy.

1) CONTRACTING WITH ONLINE OR THIRD-PARTY SERVICE PROVIDERS:

If a district contracts with a third-party company to provide external services to assist with internal needs, the third-party company must follow the same FERPA protections as required for school officials.[xxix] Some examples of these basic services could include email, calendaring, web-search, and document collaboration software. The district would set up the user accounts using basic enrollment information (name, grade, etc.) from student records. Under FERPA regulations, the provider may not use data about individual student preferences taken from student content to target ads to individual students for products, because using the data for these purposes was not authorized by the district and does not constitute a legitimate educational interest as specified in the district's annual notification of FERPA rights.[xxx]

2) ACCESS TO RESEARCH AND SURVEYING IN LOCAL SCHOOLS:

Metro Nashville Public Schools is one example of how local district policies can mirror the best practices used in Tennessee's process for approval of research or surveys. For example, if an external group would like to conduct literacy research or distribute surveys, MNPS's policy outlines specific procedures related to data use. This includes a review of research requests by a Research/ Survey Review Committee comprising the district's top leadership and research staff. Further, MNPS policy outlines the rights of parents related to research which includes:[xxxi]

- Parental right to inspect all materials that will be used in surveys, focus groups, interviews, tests, or other research instruments.
- The right to opt their child out of participation in any survey, focus group, interview, or other research-related activity.
- A list of topics that require parental consent to survey or research. These topics include questions related to political/ religious affiliation, psychological problems, sexual behavior/attitudes, anti-social or demeaning behavior, critical appraisals of family members, or legally privileged relations.

3) STATE LEGISLATION ON DATA PRIVACY AND USE:

Given the importance of student data privacy and use, a number of states have either recently passed or are working on legislation on this topic. In 2013, Oklahoma passed the "Student Data Accessibility, Transparency and Accountability Act." In 2014, Idaho passed a similar measure. The key components of both pieces of legislation are outlined below:

The Oklahoma legislation established procedures and safeguards for the Oklahoma Department of Education related to student data privacy and use. Further, it requires the Oklahoma State Board of Education to publicly develop policies and establish safeguards for student data. The legislation specifically:[xxxii]

- Requires creation of a statewide student data security plan.
- Limits the data that can be collected about individual students and sets policies regulating how that information can be shared.
- Establishes new limits on the transfer of student data to federal, state, or local agencies, as well as organizations outside Oklahoma.
- Restricts the state from requesting delinquency records, criminal records, medical records, Social Security numbers, and biometric information as part of student data collected from local schools and districts.

3) STATE LEGISLATION ON DATA PRIVACY AND USE: *(cont.)*

Though a key component of the Oklahoma legislation is the protection of student privacy, the measure also establishes new strict limits on the transfer of student data, including de-identified data, to federal, state, or local agencies and organizations outside Oklahoma.[xxxiii] This clause can hamper the ability of educators to use state and district agencies or outside organizations to analyze this information on their behalf.

Similarly, Idaho's legislation established procedures and safeguards for the Idaho Department of Education related to student data privacy and use. Further, it requires the Idaho State Board of Education to regulate data collection and publicly develop policies to establish safeguards for student data. The legislation specifically requires:[xxxiv]

- Setting student data security policies in all Idaho school districts.
- Creation of a data inventory and index.
- Enforcement of privacy protections for third-party vendors, including court action and civil penalties up to $50,000 for violations.
- Notification to the Governor or Legislature from the state board of education, which has to file annual reports about what types of student data are being collected and any breaches in data security.

Key components of the Idaho legislation are the use of data security policies in every district and use of civil penalties for violation. One different component in the Idaho legislation is the lack of a Chief Privacy Officer. State CPOs can expand districts' capacity to ensure student data privacy. The CPO and staff can aid districts with training of their employees and provide a model for their own data privacy policies.

4) RECENT LEGISLATION IN TENNESSEE:

In 2014, the Tennessee General Assembly passed legislation increasing state protections for student data privacy. The measure contains several components that are similar to legislation passed in Idaho and Oklahoma. Specifically, the State Board of Education is charged with the following tasks:[xxxv]

- Creating a publicly available data inventory along with the purpose or reason for inclusion in the data system.
- Developing publicly available district and state policies to comply with FERPA, Tennessee Code and other privacy-related statutes, regulations, and policies.

Strict regulations on the contracts governing third-party agreements are also included, along with prohibitions on collecting student data related to (1) political affiliation; (2) religion; (3) voting history; and (4) firearms ownership.

A key component of the Tennessee legislation is the enhanced protection of de-identified student data within third-party contracts that still allow districts and schools to use data for educational improvement. Further, the TDOE is required to develop a model student records policy for districts including: annual notification of parental right to request student information; security when providing student data to parents or guardians; and a plan to allow parents and guardians to view online, download, and transmit data specific to their children's educational records. This legislation is designed to ensure the protection of student data within the effective use of educational information.

RECOMMENDATIONS

As noted in the table on the previous page, a few additions to Tennessee's current data privacy policies can enhance protections and the use of data for educational improvement. Research demonstrates that the use of data allows teachers and schools to improve student achievement, and it helps close the achievement gap. It is important for Tennessee state policies to keep the interests of students in mind by protecting privacy and still allowing data collection, use, and research to occur for educational improvement. Below are key practices to include in data-related policies and common pitfalls to avoid.

KEY PRACTICES

Communicate transparently with the public. The Tennessee Department of Education, local school districts, schools, and stakeholder organizations must explain how data can enhance personalized learning for students. These organizations also must outline the "who, what, when and where" of data collection when sharing information with the public. This communication with stakeholders will help to dispel myths and clarify the value of data. For example, as the TDOE begins a new initiative, the amount of data collection and other related issues should be communicated proactively to the public.

State the purposes of the state's data and privacy policies. Including an acknowledgment of the educational value of data and the importance of privacy and security safeguards expresses a clear commitment to smart education data usage and privacy. Further, a well-designed purpose statement will guide state and local leaders in implementing policies and show the importance of communicating effectively with parents about these important, but complex issues.[xxxvii]

KEY PRACTICES	COMMON PITFALLS
COMMUNICATE TRANSPARENTLY WITH THE PUBLIC.	LIMITING THE USE OF DE-IDENTIFIED DATA WHICH MASKS STUDENT IDENTITY.
STATE THE PURPOSES OF THE STATE'S PRIVACY POLICIES.	EXPRESSLY PROHIBITING THE SHARING OF DATA WITH THIRD PARTIES.
CONSIDER FERPA PROTECTIONS WITHIN TENNESSEE LAW.	ADOPTING REGULATORY OR STATUTORY LANGUAGE THAT PREVENTS USEFUL DATA PRACTICES FROM OCCURRING.
CREATE A DATA INVENTORY AND THE ABILITY TO REVISE WHAT DATA IS COLLECTED.	
FOCUS ON LOCAL DISTRICT TRAINING AND CAPACITY.	
IMPOSE CIVIL PENALTIES FOR MISUSE.	
CREATE A CHIEF PRIVACY OFFICER.	

Consider FERPA protections within Tennessee law. FERPA is a federal law created in 1974 for the purposes of protecting student data and privacy. Tennessee is, and will continue to be, required to comply with the provisions in FERPA in order to be eligible to receive federal education dollars. As such, it is important that any future legislation complement FERPA.

Create an annually updated data inventory and the ability to revise what data is collected. A running list of data collected at the state and district levels should be updated annually and communicated widely. Additionally, language should be added that assigns responsibility to state agencies for coordinating data. This should include eliminating data that is collected for no purpose or reason. This will give parents a clear picture of what information is being collected about their students.

Focus on local district training and capacity. It is important to remember the purpose of collecting student data – to make better informed decisions about individual students' educational experience. The state should provide more support and training for school districts as they develop local policies related to data privacy and use. For example, the US Department of Education has created a Privacy Technical Assistance Center (PTAC) that provides guidance and best practices on protecting students' identifiable information. PTAC recently released guidance for protection of online student data and provided a breakdown of FERPA regulations.[xxxviii] The TDOE, under the direction of the Chief Privacy Officer (see below), could provide targeted training sessions for district and school leaders and additional resources in the current CORE offices.

Impose civil penalties for misuse of student data. Further protections of student information can include civil penalties for the misuse of data or violation of privacy agreements. Some states, like Idaho, have included this language to ensure that third parties, who are integral to many districts' data practices, must adhere to strict privacy standards and lawful uses of student data.[xxxix]

Create a Chief Privacy Officer (CPO). States like Oklahoma have required that an official within the department of education oversee the implementation of the state's student privacy policies. With limited resources, districts often rely on the use of third-party organizations to perform educational and school-related functions. Assistance from the state CPO would expand districts' capacity to ensure student data privacy. The CPO should also aid districts with training of their employees and provide a model for their own data privacy policies, considering the following recommendations:[xl]

- **Transparency:** Information on cloud service providers should be available on district websites. Additionally, parental notice should be given of these services and the types of student information that is transferred to third parties. For example, the Houston Independent School District website provided this information online to help parents learn more about the types of information that is collected about their children on websites commonly used in the district.[xli]
- **Awareness of federal, state, tribal, or local laws:** Several laws pertain to student data privacy (FERPA, COPPA, PPRA, etc.). These laws include requirements for providing online educational services to children under certain age restrictions and outlines parental and student rights.
- **Inventory of all online educational services:** Include the Terms of Service agreements for each program. Consider a process for approval of classroom-based services and communication with teachers. The Consortium for School Networking (CoSN), with support from Harvard Law School's Cyberlaw Clinic, recently released guidance on this topic.[xlii]
- **Service agreements:** Ensure that all cloud and third-party service agreements give the district "direct control" of all student information. Properly document with all appendices and incorporated documents.

PITFALLS TO AVOID

Limiting the use of de-identified data. In Tennessee and many other states, students are issued a "Unique Student ID" number which allows for their identities to be protected while schools perform daily educational and operational functions with this information. Limiting or prohibiting the use of de-identified data or the "Unique Student ID" can leave educators and researchers without the ability to analyze the information collected—rendering data collection useless.

Expressly prohibiting the sharing of data with third parties. Districts often contract with third-party organizations to provide food services, transportation, and other school-related operations. Policies that do not allow schools to share student information with these parties to perform normal functions disrupt the daily operations of schools.

Adopting statutory language that prevents useful data practices from occurring. This can be destructive for the educational use of data. For example, language like this could hamper the work that is being done with successful data use: "The department shall not disclose student personally identifiable data to any individual, organization, government, or government entity." Since the key to effective data usage and analysis in schools relies on the ability to connect information to specific students, a policy like this would interfere with educators' ability to use data to enhance student learning.

CONCLUSION

As Tennessee continues to strive for higher student achievement, effective usage of student data is integral to success, and the security of this information should be a priority. Current policies safeguard student data and protect student privacy, but should be updated to include protections for technological advances. With these concerns in mind, Tennessee policymakers must carefully consider what is best for every student. It is important that the right data be collected for the right reasons and for the right purpose. Tennessee has the opportunity to both protect students' privacy and advance tools that can dramatically improve the educational experience of all Tennessee students.

SCORE 1207 18th Avenue South, Suite 326, Nashville, TN 37212 — tel 615.727.1545 — fax 615.727.1569 — **www.tnscore.org**