Talking about the Facts of Education Data with School Board Members

The Data Quality Campaign and the National School Boards Association's Center for Public Education prepared this document to help school board members respond to questions about education data, explain its importance to improving school and student performance, and understand how boards can help ensure student privacy.

Data Collection and the Value of Education Data

QUESTION: Why do school districts collect data on students?
ANSWER: Data help teachers, parents, and students identify what students have accomplished and how they can improve. Aggregate data inform school leaders and the public about school and district performance.

There are two main purposes for collecting student data:

- **Continuous improvement**. Individual student data is vital information for teachers, parents and students to help them plan and target instruction more effectively. School boards need to make sure this data is available in usable formats; at the same time, they need to guarantee that access is restricted to those who need it and student privacy is protected.
- Compliance and accountability. School districts are required to collect some types of data related to state and federally funded education programs like No Child Left Behind (NCLB) and the Individuals with Disabilities Act (IDEA) to show taxpayers that their dollars are well spent and getting the intended results. In general, the U.S. Department of Education is forbidden from collecting student data and cannot look at the data about individual students that states collect. School boards should also share school and district data locally as part of fulfilling their compact with the community. Data for these purposes are combined and only reported by group, for example, by student demographic groups or school buildings.

QUESTION: What student data do school districts typically collect?
ANSWER: School districts collect academic information about students in order to understand how to best serve their educational needs.

Schools collect information such as grades, program participation, demographics, and attendance to personalize instruction and guide local decisionmaking. The Center for Public Education provides a tool at www.data-first.org for examining a range of school data as a gauge of school quality. School boards should be aware of the various types of data, and set policy for how it is to be used and who has access to it.

QUESTION: Is there a data collection component to the Common Core standards?
ANSWER: No. Common Core is simply a set of grade-level expectations and does not require the collection of any data.

Common Core and its related assessments **do not** require any new federal or state data collection and **do not** require the sharing of individual student data among states or with the federal government. In addition, the US Department of Education **cannot** collect personally identifiable information on individual students as a part of its annual reporting requirements. The Department does not have access to any of the personally identifiable information in state data systems.

QUESTION: Who has access to student data?
ANSWER: Access is role-based, which means that only teachers and other designated local personnel have access to individual student data.

In addition to a student's teachers, other authorized personnel could include school administrators and guidance counselors. Others typically only have access to aggregated, or combined, student data so that personally identifiable information is not seen. If state policy allows, exceptions may be granted for organizations evaluating or auditing federal and state-supported programs and implementing school and district accountability; organizations conducting research to improve instruction; or maintaining a teacher identification system that links teacher and students. State and federal laws prohibit disclosure of personally identifiable information about students without parental permission except in limited circumstances, for example, sharing student data with a student's new school, or designating a trusted partner as a "school official" to perform an institutional service. Any disclosure of student data by these entities may result in sanctions, including the loss of funds or a ban from receiving data in the future.

Board Members' Role in Safeguarding Student Data

QUESTION: What can school board members do to protect student privacy in their districts?
ANSWER: School boards can create policies and provide resources to support good local data use practices.

School boards have a critical role in ensuring student data privacy and security. At the local level, board members can:

- Ensure that teachers and school administrators are using the data storage and analysis tools provided by the state or district. Districts need to look into the extent to which schools and teachers are using free applications like Dropbox and Google Docs and create policies and governance to ensure that sufficient protections are in place.
- Create a data governance team within the district to recommend policies and best practices related to data use.
- Advocate for resources to support student privacy in your district like training, technical assistance, and data coaches to help teachers and school leaders use data properly and effectively.
- Communicate with parents and the public about the value of data and what your district is doing to ensure that student privacy is protected. Engage community participation in forming data policies, for example, by conducting surveys or including parent representation on committees.

QUESTION: How can school board members act with regard to their state's privacy policies?
ANSWER: School board members can play an important role by ensuring compliance with state privacy laws and advocating for consistent policies and supports across the state.

School boards can develop effective local privacy policies, ensure compliance with state and federal policies, and advocate for consistent statewide policies. While federal law sets limits on how personally identifiable data (i.e., name, place and date of birth, Social Security number, or any other information that could be used to distinguish an individual's identity) can be accessed and shared, states also have their own policies and practices designed to ensure the privacy and confidentiality of data including laws that address data security and security breaches, laws that limit who has access to student data, and governance bodies charged with monitoring student data collection and protecting privacy. School board members can ensure that these state policies are being followed within their district and that local policies align with state privacy and security protections. Board members can also talk with state policymakers about the importance of state legal and technical supports in safeguarding data at the local level and about the need for consistent privacy policies across the state.

QUESTION: How can school board members talk with state policymakers about privacy?
ANSWER: School board members can advocate for secure data systems and for the effective and safe use of data.

States have the scale and buying power to provide the type of secure, customizable data system that many districts do not have the funding or expertise to implement independently. If your state does not already provide such a system, talk with your policymakers about the importance of state support for secure data use and their role in ensuring that privacy policies are consistent across the state. Also, make sure your policymakers know the many uses of data that are permissible under law and advocate for these data to be used to create high school feedback reports, school report cards, early warning systems, a teacher-student data link, and other resources and reports that can be used for research to improve instruction.

Data Privacy and Working with Service Providers

QUESTION: What services do service providers offer and how is privacy protected when states and districts work with service providers?
ANSWER: Most states and districts rely on trusted service providers to manage some aspect of their data systems. There are numerous federal and state laws that limit how service providers can use the data they are contracted to manage. Service providers are prohibited from using or disclosing personally identifiable student information for commercial purposes without parental consent.

Out of necessity, states and districts have always contracted with external partners to securely manage, analyze, and store their data so that they can provide timely, meaningful, and useful information to the parents, teachers, school leaders, and policymakers who need it to improve student achievement. In doing so, states and school districts are required to take steps to protect the data and must adhere to federal and state laws protecting student privacy. Contracts with vendors should be clear that states and districts retain ownership of all data and service providers are prohibited from using the data in any way they are not specifically authorized to do. In addition, federal law requires that any individual or entity that a state or district authorized to access its education data must:

1. Use student data only for authorized purposes;
2. Protect the data from further disclosure or other uses; and
3. Destroy the data when it's no longer needed for the authorized purpose.

School boards should work closely with their school attorney when contracting with service providers to make sure student privacy is protected and to ensure that state and federal laws are followed.

QUESTION: How did the 2008 and 2011 Family Educational Rights and Privacy Act (FERPA) regulations affect the law?
ANSWER: These regulations sought to clarify the law in response to direct requests from states and did not weaken the law. In fact, the regulations established new provisions to strengthen implementation.

FERPA is a federal law that limits when education agencies like schools can disclose personally identifiable information about students kept in their education records. In 2008 and 2011, the federal government released regulations as a response to state requests for clarification regarding the role of the state in using student data while maintaining privacy protections around personally identifiable information. These regulations were accompanied by provisions designed to tighten privacy protections and enforce FERPA more fully (e.g., the establishment of the Privacy Technical Assistance Center (PTAC) through the Department of Education, the creation of a Chief Privacy Officer for education data, and the implementation of penalties associated with privacy lapses).