Student Data Collection, Access, and Storage

Separating Fact from Fiction

Issue Overview

Student data collected by districts and states can be a powerful tool for families, educators, and education leaders to support student learning. Each of these groups benefits from education data, but they do not need the same data. District and state data systems are constructed to ensure that individuals can access only the data that are appropriate for their role. Still, questions from the public about how these data systems work and how student privacy is protected have been increasing. **A recurring concern is the feared existence of a "permanent record"—a single, lasting repository of a student's academic, behavioral, and administrative data that potentially could be used to harm the student.** The public lacks clarity as to what data are collected by districts and shared with other entities, which has led to concerns about access to student information. As a result, state policymakers may be faced with questions about the content, funding, use, and security of their state information systems, such as statewide longitudinal data systems.

The Facts

"Permanent records" do not exist in the form that is often characterized in public conversations about student data privacy. There is no single, lasting record containing multiple types of student data that could be inappropriately accessed and used to limit a student's future opportunities.

🔒 **Disciplinary, health, and financial data are not stored in a single location** linked to an individual student; therefore, no individual or entity has access to all of this sensitive information.

🔒 **Employers and the media cannot, by law, access individual student records** unless consent is given by the student or the parent (if the student is under 18 years old).

🔒 **The US Department of Education is prohibited by law from creating a federal database** with students' personally identifiable information (e.g., information such as Social Security numbers).

The effective, meaningful use of education data to improve student achievement requires proper safeguards to ensure the safety and security of these data. Over the past year student data privacy has emerged as a prominent theme in policy, media, and political conversations. This attention has revealed a need for additional knowledge and clear information about the laws, policies, and procedures that govern student information practices. The Data Quality Campaign's *Safeguarding Data Briefs for Policymakers* provide key facts and recommendations that address high-priority issues that have characterized these conversations.
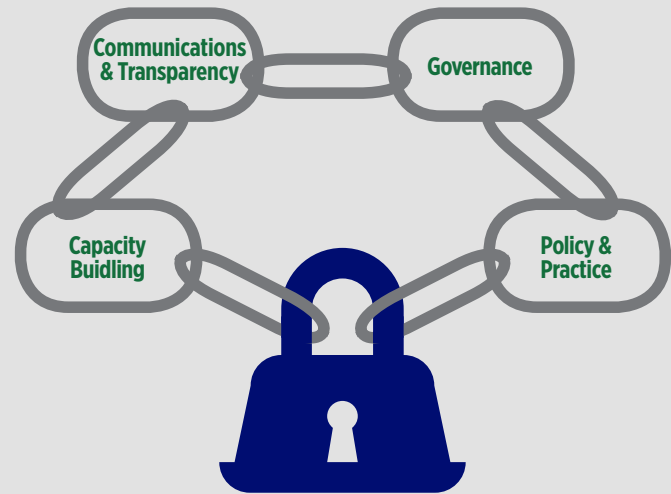
In *The Proverbial "Permanent Record,"* Elana Zeide, privacy research fellow at New York University's Information Law Institute, finds that **"public educational institutions and agencies have not created a 'permanent record' where individuals can access students' education histories at a keystroke."** She concludes that these institutions and agencies need to implement additional policies and protections to ensure that the information they do collect is safely and responsibly managed and is used only to further students' educational interests and to improve education systems.

A group of education and privacy experts came together to discuss the implications of this paper's findings for the education field. They developed the enclosed recommendations for policymakers. (See last page for contributors.)

⚿ **States and districts provide role-based access to students' personally identifiable information** so that only authorized users can access the data they need to do their jobs.

⚿ **States collect from districts a small subset of information about students.** States need to retain limited information about students after they leave the system; these data are not used to penalize individuals but to allow states to understand educational and workforce trajectories and support successful pathways.

⚿ **States have policies regarding data storage and retention** that dictate how long data can be stored and when they should be destroyed.

⚿ The **Family Educational Rights and Privacy Act requires** third-party service providers working on behalf of states and districts to (1) **use student data only for authorized purposes;** (2) **protect the data from further disclosure or other uses;** and (3) **destroy the data** when no longer needed for the authorized purposes.

Recommendations for Policymakers

Given the concerns that have been raised about the security and privacy of records—both those of current students and those maintained after a student leaves the system—the Data Quality Campaign and its partners recommend that state and federal policymakers take action in the four following areas:

Communications & Transparency

Governance

Capacity Buidling

Policy & Practice

I. PRIORITIZE COMMUNICATIONS AND TRANSPARENCY

⚿ **Communicate the value of collecting data,** including the following information:

- why it is necessary and appropriate for individual-level data to be maintained in statewide longitudinal data systems and how these data can be used to create valuable resources such as feedback reports and program analyses

- the value of linking data over time and across the early childhood, K–12, postsecondary, and workforce systems

- that only necessary data are being collected by states and that access to data about individual students is limited to those who need it to do their jobs

- why some data must stay in the system after an individual's departure from the system to ensure that the state can evaluate and improve educational and workforce pathways

⚿ **Create resources to clarify the flow of data** in your state that can be accessed and understood by anyone and clearly communicate the following information:

- that parents have a right to view the data being collected about their child

- what types of data are collected about students and who authorizes that collection

- what school-level data are shared with districts, states, and the federal government and what form the data are shared in

- what data are linked between the state's early childhood, K–12, postsecondary, and workforce systems and who has access to those data

- whether data shared at each level (school, district, state, and federal) are personally identifiable, associated with a unique student identifier, de-identified, or aggregated

- permissible activities of those internal personnel and external entities who have access to a particular type of student information

- purposes served by disclosures to third parties, including data management, analysis, and safeguarding

II. ESTABLISH GOVERNANCE

🔒 **Establish and strengthen data governance structures within agencies and across the P–20/workforce (P–20W) system** by creating the following:

- a systematic governance body across P–20W agencies that is empowered to make necessary data-related decisions, including what data are linked across agencies; is empowered to implement changes; and is sustainable

- formal roles and responsibilities for officials and staff involved in managing data at the state, district, and local levels (including the creation of a state chief privacy officer)

- procedures to minimize the storage of personally identifiable information and the risk of data breaches, including data minimization rules, data de-identification practices, data destruction policies, and privacy and security best practices

- criteria for approval of data sharing and access requests within the state by researchers and other entities

- procedures for auditing data privacy and security measures and processes for correcting any problems

III. REVIEW AND UPDATE PRIVACY AND SECURITY POLICIES AND PRACTICES

🔒 **Review current federal and state laws** that govern data collection, retention, and destruction and take the following steps:

- Educate practitioners and educators about these laws and the protections already in place.

- Provide supports to promote quality implementation.

- Identify areas where state policy can supplement federal law, and work to enact these policies.

- Establish civil penalties for the misuse of student data.

🔒 **Develop and implement data destruction policies** that address the following issues:

- procedures for destruction in all places where education data are stored at the state level

- guidelines for how long and in what manner data should be kept to ensure their availability for legitimate educational purposes

- processes for tracking and monitoring data destruction

- consequences for violating policies

- guidelines for de-identification of personally identifiable information

IV. BUILD STATE AND LOCAL CAPACITY TO SAFEGUARD DATA

🔒 **Require all contracts with service providers at the state and district levels to contain explicit information about that provider's data collection, storage, and sharing practices** including the following information:

- specific services to be provided

- data the service provider receives for the purpose of executing contracted services

- provider's permissible uses of student data

- a statement articulating that the service provider does not own the data it manages or analyzes

- retention limits and destruction requirements

🔒 **Provide model contract language** with these provisions included for district use.

🔒 **Require all state or district contracts with third-party service providers to be available online** so that the public can view them.

Related Resources

🔒 *The Proverbial "Permanent Record"* (Elana Zeide)

🔒 "Who Uses Student Data" graphic and video (Data Quality Campaign)

🔒 *Pivotal Role of Policymakers as Leaders of P–20/ Workforce Data Governance* (Data Quality Campaign)

🔒 Colorado Department of Education Data Privacy and Security Page

🔒 *Data in the Cloud: A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era* (National School Boards Association)

🔒 Best Practices for Data Destruction (US Department of Education Privacy Technical Assistance Center)

🔒 Data Privacy Toolkit (US Department of Education Privacy Technical Assistance Center)

For more Data Quality Campaign resources on privacy, security, and confidentiality visit www.dataqualitycampaign.org/action-issues/privacy-security-confidentiality.

This brief was developed with contributions from the following individuals:

John Bailey
Foundation for Excellence
in Education

Richard Contartesi
Loudoun County Public Schools

Dan Domagala
Colorado Department of Education

Joseph Jerome
Future of Privacy Forum

Keith Krueger
Consortium for School Networking

Reg Leichty
Education Counsel, LLC

Greg Mortimer
Denver Public Schools

Jules Polonetsky
Future of Privacy Forum

Jim Siegl
Fairfax County Public Schools

Chip Slaven
Alliance for Excellent Education

Omer Tene
International Association of
Privacy Professionals

Amelia Vance
National Association of State
Boards of Education

Elana Zeide
New York University's
Information Law Institute

The Data Quality Campaign will continue to engage the education and privacy communities to learn from each other and provide useful guidance to policymakers and practitioners on how to effectively use education data while safeguarding them.