Safeguarding DATA
Briefs for Policymakers

DQC DATA QUALITY CAMPAIGN
Using Data to Improve Student Achievement

Student Data and Consent Policies

Avoiding Unintended Consequences

Issue Overview

Effective use of education data to improve student achievement requires that data are safe and secure. Parents should be able to understand what data are collected about their child, how those data are used and shared, and how the data are protected. Parents and privacy advocates have expressed concern about the amount of data collected in schools today, in many cases because they do not trust that the data collected will be valuable or useful to students or that the data will be kept safe.

High-quality education data can empower parents to better understand their child's academic progress and play a greater role in their child's education. Current law requires that parents have access to the data in their child's education record. Some have advocated for policies that allow parents to have more choice, specifically the ability to "opt out," when it comes to what data are collected, used, and shared about their child. Yet including more consent allowances could make it more difficult for parents to receive information about their child's progress and could disrupt other core school and district activities. This disruption could create significant teaching and administrative burdens or lead to unintended consequences for schools and families.

To the extent feasible, parental choice policies should be structured according to the use of the data in question. Schools use data for different purposes, which have different degrees of impact on a student's educational experience: administrative, instructional, assessment and measurement, and optional/noneducational. Parents should have more choice for activities in which opting out will not have a negative impact on their child's education, like data collection for noneducational purposes such as marketing for yearbooks or class rings. **It is not feasible, however, to allow parents to limit the data schools collect about their child for administrative, instructional, or assessment and measurement purposes** because it would hinder or minimize the impact of data's use to improve student achievement and would strain everyday school functions.

Policy leaders need to understand the potential implications of enacting such policies and be prepared to help parents understand this issue.

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 *Student Data: Trust, Transparency, and the Role of Consent,* the Future of Privacy Forum finds that increasing allowances for parental consent, namely a parent's right to "opt out," in education information practices should depend on the use of the data in question. Opt-out policies, when applied to all instances in which data are collected in schools, could interrupt activities that are central to a student's education. The authors conclude that "rules around notice and choice must balance individuals' right to privacy with organizations' need to collect, use, and share personal information for normal business purposes. … **Only when student data can be used for non-educational purposes should choice be mandated."**

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.)

Type of Use	Example	Is Choice Required?	Should Additional Notice and Transparency Be Provided to Parents?
Administrative	Course scheduling, school busing	No	No
Instructional	Online homework, learning apps	No	Yes
Assessment and Measurement	Standardized tests, course assessments	No	Yes
Optional/Noneducational	School yearbooks, PTA fundraising	Yes	Yes

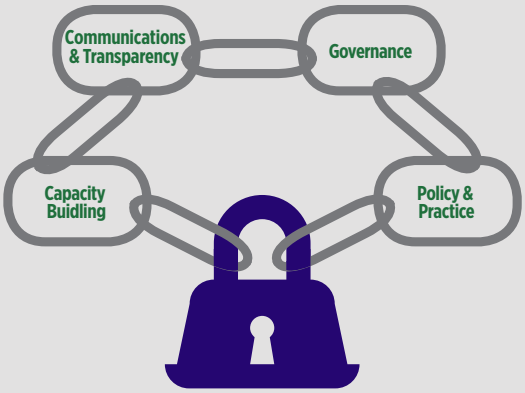
Source: Future of Privacy Forum, *Student Data: Trust, Transparency, and the Role of Consent*

The Facts

- Requiring parental consent before any party can collect, access, or use student data for instructional, administrative, or assessment and measurement purposes could weaken the quality of the student learning experience, reduce efficiency, and increase workload for teachers and administrators. For example, **requiring parental consent** could have the following effects:
  - **Limit parents' ability to get information** on student progress throughout the school year, such as through online data dashboards.
  - **Diminish the quality of personalized instruction** for students with exempted data. Teachers may have to divide classrooms by students who are permitted to use certain educational tools and those who are not. Teachers may also have to store information, such as student assessment results, in a separate, manually maintained information system. Using a separate system could make the data less secure and more difficult to use for intervention strategies.
  - **Reduce valuable classroom instructional time** by increasing teacher and administrator workload for basic tasks. School administrators and teachers may have to conduct administrative tasks by hand and/or manage multiple systems to provide basic services, which would create software design challenges.
  - **Weaken the security of data management tools or email systems used in schools.** Schools may be forced to build their own data management tools or run their own email systems, which may be less secure than those services provided by outside parties with greater technical expertise and capacity.
  - **Severely limit state and local officials' ability to evaluate educational programs** by taking into account student performance, due to incomplete datasets, and thus **limit the public's ability to access information on the quality of educational programs that receive public funding.**
- Parents have the right to review their child's information. The Family Educational Rights and Privacy Act gives parents the right to access and challenge incorrect school records about their child.
  - The law requires written consent to disclose student data contained in an educational record, with exceptions for certain situations and enumerated entities, including those who are designated as school officials or those who are conducting audits or evaluation of educational programs.
  - Schools can share directory information without parental consent, but they must inform parents as to what information is considered to be "directory" and provide parents with the option to opt out of this sharing.
- Requiring parental consent in more cases could increase achievement gaps between students of different socioeconomic backgrounds. The Future of Privacy Forum argues that allowing parents to opt out of—or requiring them to opt in to—technology-driven learning activities could prevent low-income students from being able to access the same tools as their peers attending affluent public or private schools with significantly more available resources.

Recommendations for Policymakers

One of the most important uses of data is to empower parents with information to ensure that their child is getting what he or she needs. To address parents' concerns about data collection, sharing, and use, while allowing for the effective use of education data to improve student achievement, the Data Quality Campaign and its partners recommend that state and federal policymakers take action in the four following areas:



I. PRIORITIZE COMMUNICATIONS AND TRANSPARENCY

- **Create ways for parents and the public to learn why data are collected and shared and why these activities are good for students,** including why it is necessary for a student's data to be collected and used for administrative, instructional, and assessment and measurement purposes.
- **Clearly communicate to parents that they have a right to view the data being collected and instances when they have the ability to opt out of data collection in school.** Ensure that parents are aware of their rights and choices under current federal and state law by making this information easily accessible and easy to understand.
- **Create a public list of the types of third-party service providers** with whom data are shared within the state. Encourage districts to provide a list of each of the service providers they contract with and what function they serve.

II. ESTABLISH GOVERNANCE

- **Create and update data governance policies** to ensure that they cover the following issues:
  - Define clear roles and responsibilities for all who manage education data.
  - Articulate who can access what data and under what conditions.
  - Establish accountability mechanisms.
  - Recognize the shared data stewardship of the state, districts, educators, information technology managers, and other entities.
  - Require strong data security standards.

III. REVIEW AND UPDATE PRIVACY AND SECURITY POLICIES AND PRACTICES

- **Review current parental consent policies,** and determine under what conditions the opportunity to opt out of the collection of student data should be provided and when it should not.
- **Specify noneducational activities in which allowing parents to opt out of data collection is appropriate.** Encourage districts and schools to give parents the ability to choose in circumstances in which student data could be used for noneducational purposes and to include these opt-out options in contracts with third parties.
- **Distinguish between different uses of student data, and ensure that privacy and security policies properly reflect these differences.** When creating policy make clear the distinction between data collected by educational institutions and those collected by online learning tools and programs. Different uses of data require different policies.
- **Require accountable and transparent third-party relationships.**
  - Require service providers in your state to establish shared guidelines, and increase transparency about the data they collect and how the data are used.
  - Require districts to establish accountability and transparency through the contractual process, including ensuring that contracts articulate what data providers receive, permissible uses of those data, and consequences for violating contract provisions. These contracts should also include a statement that the service provider does not own the data it manages or analyzes.
  - Require all contracts with third-party service providers to be placed on the state or district website so that the public can view them.

IV. BUILD STATE AND LOCAL CAPACITY TO SAFEGUARD DATA

- **Support districts to enable them to fulfill their role in safeguarding data** by providing the following tools:
  - a training module on data privacy and security that could be offered to district leadership
  - model third-party contract language
  - guidance for districts—and educators in particular—outlining important considerations when using "click-through" agreements
  - guidance that districts can follow in the event of a data breach
  - a channel for open, ongoing communication about district responsibilities and pressing questions they have
  - resources for professional development and training for teachers and all staff

Related Resources

- *Student Data: Trust, Transparency, and the Role of Consent* (Future of Privacy Forum)
- *A Stoplight for Student Data Use* (Data Quality Campaign)
- *Supporting Early Warning Systems* (Data Quality Campaign)
- *Framing the Law & Policy Picture: A Snapshot of K–12 Cloud-Based Ed Tech & Student Privacy in Early 2014* (Berkman Center for Internet and Society, Harvard University)
- *Our Commitment to You: Clear Privacy Practices* (Consortium for School Networking)
- *Privacy and Cloud Computing in Public Schools* (Center on Law and Information Policy, Fordham Law School)
- *Policy Guidelines for Building a Student Privacy Trust Framework* (Software & Information Industry Association)

For more Data Quality Campaign privacy, security, and confidentiality resources 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

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.