

The Federal Role in Safeguarding Student Data

People need access to data. Individual students and job seekers, families, educators, communities, and policymakers must have the information they need to foster successful journeys through education and the workforce. Robust statewide longitudinal data systems (SLDSs) can be designed to prioritize meaningful access to data but must also protect individuals’ privacy. Data is a powerful tool to guide decisionmaking, and leaders must prioritize safeguarding that data.

The federal government has a role in prioritizing student data privacy and security and building trust in the appropriate use of student information. The Data Quality Campaign offers the following context to frame the discussion about what the federal government can do to safeguard student data.

Data Matters to Meeting Our Education Goals

We have more useful and richer information than ever before that can be used to support teaching and learning. But educators, students, and families will not use this information to make decisions, personalize learning, and help students succeed if they do not trust that doing so is safe. In recent years, states, districts, education and privacy organizations, and school service providers have demonstrated tremendous leadership in prioritizing the need to safeguard student information. These efforts have led to greater transparency about what data is collected and for what purposes, stronger privacy and security laws and policies, clearer governance of data, and more open communication across the field—especially with parents and teachers.

There is a critical federal role in complementing, supporting, and reinforcing these activities. **Federal action should continue to align and clarify student protections and build capacity throughout the field to protect student information.**

Existing federal laws including the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Children’s Online Privacy Protection Act (COPPA) offer an important legal foundation for safeguarding student data. Information practices and technological capabilities have changed radically since each of them was enacted. The federal government should continue to provide a clear student data privacy and security framework and support for states, local school systems, and schools that have varying legal and technical capacity.

Potential Areas for Federal Action

We believe that with federal leadership and guidance, state and local leaders and especially those closest to students—teachers and principals—can be informed about how federal laws apply to activities in the classroom

and can be empowered to use education data well and safeguard it. We propose the three general areas for federal action on the following page.

FEDERAL LAWS THAT PROTECT STUDENT INFORMATION

LEGISLATION	DATE ENACTED	ADMINISTERED BY
Family Educational Rights and Privacy Act (FERPA)	1974	US Department of Education
Protection of Pupil Rights Amendment (PPRA)	1978	US Department of Education
Children’s Online Privacy Protection Act (COPPA)	1998	Federal Trade Commission

1. Ensure that federal laws provide a strong foundation to protect student information in a constantly changing and increasingly digital school environment.

THE CURRENT LANDSCAPE: Current federal laws do not specifically address current and evolving technology-driven practices that have implications for the privacy and security of student information. Student data is now collected, stored, and shared digitally—rather than on paper—often in cloud-based systems. New technologies can produce more sophisticated feedback on student progress and are informing classroom practices and educators’ efforts to personalize instruction. While COPPA addresses online privacy, how the law applies to the use of various technologies in the classroom is not always clear to school districts and educators. And while FERPA has been applied to electronic records in some situations, the law is not designed to cover data collected outside of a student’s official school record. Neither law addresses current and

potential security concerns related to the aforementioned new digital capabilities.

THE FEDERAL ROLE: Federal law should establish a strong privacy and security foundation for educational institutions and agencies that provides baseline protections and consistency across states. Yet federal law should be broad enough to allow states and districts to innovate and respond to new developments in technology. Any changes to FERPA should recognize the electronic environments in which student data is generated and stored, account for schools’ uses of third-party online applications that collect student information, and address the need for security safeguards designed for modern digital environments.

2. Ensure that the federal government coordinates across agencies to provide clarity to those on the ground as to how privacy laws work together.

THE CURRENT LANDSCAPE: States and districts must navigate the student data privacy protections offered by federal laws, namely FERPA and PPRA, which are administered by the US Department of Education (ED), and COPPA, which is administered by the Federal Trade Commission (FTC). An aligned federal foundation that is coherent across applications and a continued commitment to coordinated communications can provide consistent definitions and standards for those on the ground.

THE FEDERAL ROLE: ED and the FTC should continue to coordinate to meet the needs of families, educators, and others working in states and school systems. These agencies can issue joint guidance to help individuals in states and districts navigate and implement federal privacy laws and inform complementary state laws and policies. They can help clarify for the public which federal laws govern student data privacy, their application in school settings, and federal governance of websites and online applications.

3. Support state and local capacity to safeguard data.

THE CURRENT LANDSCAPE: To safeguard student data, individuals in schools and local school systems need training and support to build a culture of trust and implement best practices in data privacy and security. The federal government has numerous tools to support local infrastructure and capacity building. Federal agencies have already taken steps to support the field; the Privacy Technical Assistance Center (PTAC), for example, has provided great value to the field through its hotline and its guidance on such important issues as data breach response and model terms of service.

THE FEDERAL ROLE: Continued federal attention to the role of states and school districts in safeguarding student data is vital. The federal government can do more to

support them by providing more tools and resources to help them adopt policies and best practices in transparency, governance, and privacy and security. These supports can also include funding for building capacity—especially through related training and professional development—throughout the system, from the state to the local, school, and classroom levels. To provide leaders more direct, real-time technical assistance (TA) and guidance, the federal government should make additional investments in the PTAC and consider additional federal privacy TA centers. There are also opportunities in federal law to address the need to equip teachers and school leaders to protect and use data effectively.



The Data Quality Campaign is a nonprofit policy and advocacy organization leading the effort to ensure that data works for everyone navigating their education and workforce journeys. For more information, go to dataqualitycampaign.org and follow us on [Facebook](#) and [Twitter](#).