DQC FERPA Recommendations

April 2023

Parents, teachers, and state leaders use education data every day to make decisions in support of student success. That information must be safeguarded and used responsibly and ethically. The federal government has a critical role to play in safeguarding student data—it is uniquely positioned to ensure that federal laws provide a strong foundation to protect student information, coordinate across federal agencies to provide clarity as to how privacy laws work together, and support state and local capacity to safeguard data.

The foundational federal education data privacy law is the Family Educational Rights and Privacy Act (FERPA), which was first enacted in 1974. FERPA ensures that the privacy of students' education records is protected and that families have rights to review their children's information. However, the education landscape has changed dramatically since FERPA was last amended in 2002. The US Department of Education (ED) has modernized FERPA regulations, which include critical updates to the law's implementation. States have passed numerous student data privacy laws (146 laws across 47 states since 2013) that build on the foundation of FERPA. Additionally, technology has evolved and exists in the classroom in ways that Congress could not have anticipated. As a result, FERPA would benefit from improvements that support state autonomy and continue to ensure the rights of students and parents while also providing an effective privacy framework aligned to current practice. In short, to continue encouraging effective data use while protecting the privacy of people's information, FERPA must be strengthened in the following ways:

- Codify the 2008 and 2011 regulations;
- Build state and local capacity to protect student privacy;
- Align FERPA's provisions with other federal privacy laws; and
- Improve privacy policy and practices transparency.

Codify the 2008 and 2011 Regulations

ED has issued many regulations to strengthen and clarify FERPA since its enactment. In particular, regulations issued in 2008 and 2011 were a direct response to state requests for clarification about how to implement FERPA in the digital age and promote effective data use by states and districts. The updated FERPA regulations clarify and strengthen the law's key privacy protections (e.g., penalties for improper disclosure, requirements for reasonable methods to ensure individual data is safeguarded and used responsibly). The regulations also clarify provisions that enable the use of data to support critical education functions. For example:

- Districts can share limited data with school bus companies to ensure their students get to and from school on time and safely.
- Teachers can use apps and other education technologies to personalize learning in the classroom.
- School and district leaders can use electronic data systems to protect, manage, and use their data, including to inform policy and program decisions.
- States can securely link K–12 data to early childhood, postsecondary, and workforce data to understand outcomes and provide feedback reports to schools and districts to improve their service to students and families.

Recommendation:

To ensure that schools and districts can continue to offer these and other important services while safeguards remain in place, the next FERPA must codify the 2008 and 2011 regulations.

Build State and Local Capacity to Protect Student Privacy

The landscape of student data privacy laws and policies is complex. It involves multiple federal laws and regulations, state laws, and often district policies and practices, making it challenging for people to feel confident they are implementing all requirements with fidelity. This complexity can have a chilling effect on important work to expand data access and use in support of students. Teachers and school leaders, local school systems officials, and state agency leaders need support to navigate these challenges and build a data culture that centers on individual privacy. Capacity building across all levels of government is the best way to ensure that educators and other professionals in the education system understand and can act on their responsibilities to protect data while still using it to support students and their families. The federal government can play a vital role in building capacity in states and districts by providing more technical assistance, guidance materials, and investments in training and professional development. FERPA reauthorization creates an opportunity to enable much-needed capacity building at the state and local levels.

Recommendations:

- Build capacity in states, districts, and schools by requiring training to support the use and protection of data for all staff with access to students' personally identifiable data.
- Encourage the use of existing federal program resources to support expanded privacy training for state, district, and school staff (e.g., ESEA, Title II; HEA, Title II; and ESEA, Title IV (Student Support and Academic Enrichment)).
- Improve support to state education agencies and service providers by codifying the Privacy and Technical Assistance Center (PTAC) and charging it with:
    - Continuing PTAC's efforts to produce resources, guidance, toolkits, and technical assistance that help state and local leaders untangle challenging privacy questions.
    - Expanding its scope to include technical assistance on state student data privacy laws and how they should be interpreted in connection to federal laws.

Align FERPA's Provisions with Other Federal Privacy Laws

States and districts must implement student and child data privacy protections that derive from a wide range of federal laws and are administered by different federal agencies, including the Children's Online Privacy Protection Act (COPPA), the Protection of Pupil Rights Amendment (PPRA), the Elementary and Secondary Education Act (ESEA), and the Individuals with Disabilities Education Act (IDEA). Consumer privacy laws, while not necessarily education specific, have implications for education technology and can create the potential for additional privacy requirements schools and districts must abide by. An aligned federal foundation and a continued commitment to coordination across agencies can ensure consistent definitions and standards for those on the ground, reduce confusion and burden at the district and school levels, and enable more effective implementation of the law. Congress can use FERPA reauthorization to address some of this confusion.

Recommendations:

- Align FERPA's definitions (e.g., service provider and education record) and key provisions (e.g., opt-out opportunities) with all other federal education and privacy laws.
- Ensure that FERPA includes enough flexibility, while maintaining appropriate safeguards, to remain:
    - Relevant as technology evolves;
    - Consistent with other federal laws as they are updated; and
    - Compatible with state laws that may build on the rights and protections enumerated in FERPA.
- Coordinate with the Departments of Labor, Health and Human Services, and other relevant federal agencies to support cross-agency data efforts, including through joint guidance, technical assistance, and resources.

Improve Privacy Policy and Practices Transparency

Transparent privacy policies and practices are critical to building trust with the public, particularly parents, about the value of data. Transparency allows the public to see what is being collected, how that information is being safeguarded, and how it is being used to help students succeed. Equipped in this manner, the public is less likely to worry or have misperceptions about how data is used. In addition, seeking public participation, discussion, and input on the use and governance of data empowers parents, teachers, education and community leaders, and other stakeholders, building collaborative relationships that can be relied upon to solve problems jointly when they arise. FERPA should include provisions that improve policy and practice transparency for all, especially for families and community members.

Recommendations:

- Require districts to post on their website or otherwise widely share a description of what is considered directory information, generally how directory information is used, the right to opt out of sharing directory information, and the consequences of opting out.
- Require states to maintain and publish the types of data requests that are fulfilled and indicate what data was provided and whether the requests included personally identifiable information (PII).
- Either directly or through an outside entity, empower ED to help families and other community members understand their rights under FERPA and PPRA by:
    - Conducting public trainings (e.g., webinars) that are free of charge and directed at families.
    - Producing or revising tools that are publicly available and easily accessible that explain federal student privacy laws to families and other community members.

Conclusion

FERPA can help ensure that student data privacy is protected, parental rights are safeguarded, and states and districts are not inhibited by uncertainty. When policymakers next reauthorize FERPA, they must address not just what is needed for a few years, but for decades into the future. Updates to FERPA are rare, therefore, reauthorization must build a solid framework that supports and guides states and districts as they adapt to changing technology, changing needs, and new relationships that will enable them to harness the power of data. Ultimately, these recommended changes can both safeguard student privacy and security, and create a culture of trusted, informed education data use in service of learning.