DQC Data Quality Campaign

APRIL 2023

Centering Privacy

Data Access and Data Protection Go Hand in Hand

Any vision for data access and use is incomplete without a plan to protect individuals' privacy. As state leaders make decisions about policies that can better support individuals on their education and workforce journeys, they must ensure that they are taking steps to protect and secure data. But privacy is about much more than legal compliance. In addition to adhering to security best practices and laws, leaders at all levels must build trust with community stakeholders by providing access, ensuring responsible data use, prioritizing transparency, and demonstrating public value.

As data practices and technology evolve, policies must evolve with them. Centering privacy ensures that appropriate privacy guardrails that align with states' values and goals for data access and use are in place. **As leaders work to link data across education and the workforce, they must prioritize safeguarding data as a central consideration when designing data policies and practices.**

Policymakers can take four key steps to center privacy:

1. Establish governance;
2. Update policies;
3. Support people; and
4. Communicate clearly.

Establish governance

State leaders should establish data governance structures that create transparent processes to guide data access and use and that focus on making data a protected but available resource for the community. State leaders can establish data governance by:

- Enacting formal state policies that outline roles and responsibilities for overseeing and guaranteeing the protection of individual data that state agencies collect and use;
- Establishing a formal cross-agency data governance body charged with protecting privacy and overseeing decisions about data linked between agencies; and
- Designating a chief privacy officer accountable for safeguarding data within each state agency and ensuring that the necessary privacy guardrails are in place.

Data Governance Is Essential for Centering Privacy Over Time

The work of protecting data is not a one-time event, especially because data needs and practices are always evolving. Data governance refers to both the policies that govern data privacy and use and the formal, leadership-level body responsible for making decisions about how data linked between state agencies is connected, secured, accessed, and used to meet state education and workforce goals. While state policies are an invaluable tool for ensuring data privacy, ultimately a formal, cross-agency data governance body is needed to ensure that those policies are updated and implemented over time.

Update policies

The education and workforce landscapes are changing as state and local leaders address new and interconnected challenges facing their communities. As circumstances change, state leaders should regularly update privacy, security, and communications policies. States can anticipate evolving privacy needs by:

- Developing a process so that community leaders, advocates, and practitioners can provide feedback about privacy concerns and data needs;
- Regularly reviewing privacy policies and updating them to align with current best practices for responsible data use; and
- Creating shared interpretations of privacy laws across different agencies or local governmental entities.

What Are Data Privacy Policies?

Data privacy policies codify who is considered an authorized user, what types of data each user can access, and by what means they can access it. Data privacy policy is distinct from data security, which refers to the technological safeguards that prevent unauthorized individuals from accessing data.

Support people

State leaders should build capacity and a culture of responsible data use so that everyone with a part to play in keeping data safe and secure has the training and support they need. They can build this capacity and culture by:

- Requiring training and assistance for educators and other practitioners who must use individual data; and
- Developing and sharing model policies and tools for local agencies and institutions to use as a starting point for developing their own cultures of responsible data use.

Communicate clearly

A culture in which data is protected and used well is built on trust. Beyond establishing strong policies and practices, centering privacy means that states take steps to be transparent and clear with communities about how data is used and protected. State and local agency leaders can provide this transparency and clarity by:

- Proactively communicating about the value of data and publishing easy-to-find information on a website tailored for a general audience;
- Clarifying what data is accessible in what ways and to whom; and
- Designating a person or office that any member of the public can contact with privacy questions.

Conclusion

By focusing on governance, policy updates, capacity building, and communication, state leaders can effectively prioritize data privacy as a part of data access and use. When states have effective frameworks in place that center privacy, state and local leaders can turn their attention to using data to improve decisionmaking and support individuals.

ADDITIONAL RESOURCES

Centering Privacy: The Data Quality Campaign's website highlights several policy areas, one of which is centering privacy. This page provides an overview of what it means to center privacy and why centering privacy is an essential consideration when designing data policies and practices.

The Consumer's Guide to Data: This guide provides tools for state and district leaders, as well as other individuals, families, and communities, to help them better understand and talk about data. Stakeholders at all levels can also use the information in this resource to do their part to build public trust in data.

Data Integration Support Center (DISC) at WestEd: DISC supports public agencies in navigating the complexities of state and federal privacy and security regulations for integrated data systems through flexible, adaptable, and easily accessible resources; diverse media; expert guidance; and technical assistance.

Maintaining Trust as Data Use Changes: Student Data Privacy and the COVID-19 Crisis: This brief highlights short- and long-term actions state leaders can take to empower educators to responsibly use and safeguard data as they navigate online learning.

Roadmap for Cross-Agency Data Governance: This roadmap provides recommendations for states that are looking to develop and implement a high-quality cross-agency data governance committee.

Safeguarding Student Data in Higher Education: This resource highlights how, by establishing data privacy as an institutionwide priority and setting shared expectations for faculty and staff, higher education leaders can ensure that student data remains secure and properly used to help students succeed.

Student Data Principles: This resource—developed in partnership with a coalition of national education organizations—details 10 foundational principles for responsibly using and safeguarding students' personal information.

ABOUT THE DATA QUALITY CAMPAIGN

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.