Maintaining Trust as Data Use Changes

Student Data Privacy and the COVID-19 Crisis

DQC DATA QUALITY CAMPAIGN

Recovering from the COVID-19 crisis will take coordinated action across multiple critical issue areas from policymakers, elected officials, researchers, advocates, and other education leaders. To support these efforts, the Data Quality Campaign (DQC) has compiled a series of resources on key issue areas states must address as they map their paths forward. Leaders can refer to these resources to learn why these issues matter to their education goals, how to prioritize actions now and down the line, and where to find additional guidance.

Why Does Safeguarding Student Data Matter Right Now?

The COVID-19 crisis has raised new considerations for data security and privacy as educators use data to support students' education progress in an online environment. Over the past several years, policymakers across the country have enacted and updated policies designed to address safe data use in modern and evolving classrooms; now, changes in teaching practice are happening on an unprecedented scale and pace following the rapid transition to online learning. With the future of the pandemic uncertain, schools likely will continue to rely on some amount of online instruction for the foreseeable future. Families and educators value and use data to help make the best decisions for students, but if leaders do not safeguard data, people will lose trust in the information they are provided—and people do not use data they do not trust. States will need to move quickly to provide data privacy and security support so that educators and other stakeholders can trust data and use it responsibly. Some of the questions states must address include the following:

- How can educators keep student data safe in online environments if they are sharing and accessing data via new instructional tools?

- What information do parents need to trust that their child's data is being protected while also being used to support their child's education progress?

- How are new types of information being appropriately and securely incorporated into state and local data collections?

- What information do district leaders need to play a role in making sure that everyone involved in supporting students understands their responsibility to safeguard data?

State policymakers must clarify how federal and state privacy and security policies apply to the evolving data practices of this moment and support all districts, especially those with increasingly scarce resources, to safeguard data as they use it to make important decisions now and moving forward. To ensure that data can be used to support student progress, families must trust that their child's data is being used responsibly and securely, regardless of platform and learning environment.

What Actions Do States Need to Take to Support Student Learning and Recovery Efforts?

In their short-term response to COVID-19, state leaders must clarify existing state privacy and security policies, communicate clearly that privacy is a priority, and support districts in selecting service providers. Longer term, states should update governance practices to meet evolving needs and invest in data privacy training for practitioners.

Near-Term Priorities

- **Clarify existing policy.** State leaders should take stock of the state's privacy and security policy foundation and how it applies to the ways student data is being used right now. They should determine whether updates or supplemental policies are needed to account for online or hybrid instruction and continued uncertainty. Steps leaders can take include the following:

  - *Clarify and communicate to school and district leaders how state and federal privacy laws apply to online learning and online operators.* Especially if their state has enacted relevant laws in recent years, leaders should make clear how the laws apply to the current ways data is being used and shared during this crisis and make this information available on the state education agency's website.

  - *Reach out to district leaders, including technology administrators,* to ask them what their needs are and what new concerns they are facing related to data use and protection. Leaders should share this feedback with state peers and provide support accordingly. It's important to consider the different challenges districts may face as they figure out how to meet the needs of students in an online setting, including the readiness of their infrastructure to provide universal online instruction.

- **Offer guidance on the safe use of service providers.** District leaders are making device purchases and service selections at a faster pace than usual. Selecting service providers that adhere to data privacy and security best practices has always been a challenge for districts, so it is critical that state leaders take steps to help make these decisions more straightforward for those who are juggling multiple priorities and may not have the time or expertise to vet services adequately. Some states, like Connecticut (see sidebar), have already taken steps to help with this decisionmaking, such as issuing features to look for or curating lists of service providers that adhere to state-determined best practices.

- **Publicize their commitment to safeguarding data.** Leaders should use their bully pulpit to demonstrate that they value protecting student data. Protecting student data privacy starts with strong policies and practices, but it also requires building a culture of trust in data use. Myths and fears feed on a lack of clear information. Leaders must clearly communicate how student data is used and protected. They must make clear that the state's agency values data use and is committed to creating safe online learning environments in which data is used to help, and never harm, students.
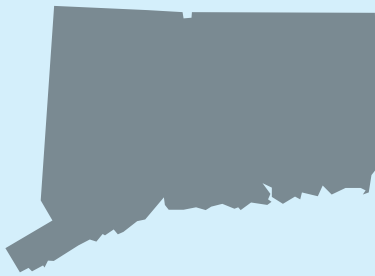
Spotlight: Connecticut

The Connecticut Department of Education published a webpage with important information related to student data privacy and COVID-19. This page includes sample emails that district leaders can send to vendors. Before the COVID-19 crisis, Connecticut took steps to help ensure that administrators and educators could select safe online tools. The state developed the "Educational Software Hub," a website that educators and district leaders can use to search for educational software developed by companies that have pledged compliance with Connecticut's privacy law.

Long-Term Considerations

- **Modernize governance policy and practices so they are sufficiently nimble in an evolving landscape.** States must ensure that their plans for crisis recovery include revisiting and strengthening data governance policies regarding safeguarding student data. During the coming years, those closest to students may need to use data in ways that policymakers do not yet anticipate. Rather than policies that govern discrete uses of data, which can quickly become outdated, data governance provides a mechanism to define processes that can address new and unforeseen challenges. Members of a governance body should be empowered to make decisions and pursue updates and clarifications to policy when needed. Specific actions states can take include the following:

  - *Work with peers across state agencies to create and maintain robust, sustainable data governance.* Leaders should ensure that the state has both K–12 data governance and cross-agency data governance practices in place. They should take steps to make this data governance sustainable, such as through codifying it in legislation.

  - *Pursue strategies to include diverse perspectives in decisionmaking.* States should revisit which stakeholders have a say in decisions about student data privacy and use. Leaders must work to include voices that represent those most affected by these decisions, including students that have been disproportionately affected by the shift to online instruction.

  - *Distribute guidance to districts.* Districts also need strong governance policies and practices. States can create new model data governance policies or share existing ones with district administrators. They should include guidance regarding how to establish and strengthen cross-agency data security practices, given that responding to COVID-19 student needs may require coordination with noneducational entities such as public health or social services.

- **Support educator and school administrator data literacy.** Training is a critical aspect of safeguarding data. Those who use student information every day have to understand how to use it safely and ethically, including while working remotely. State policymakers should include data literacy training, such as skill-building on how to protect the security of data in online environments, as part of any future investments in online learning professional development for both teachers and school administrators. Any efforts to support teachers in online learning skills should account for data use and privacy.
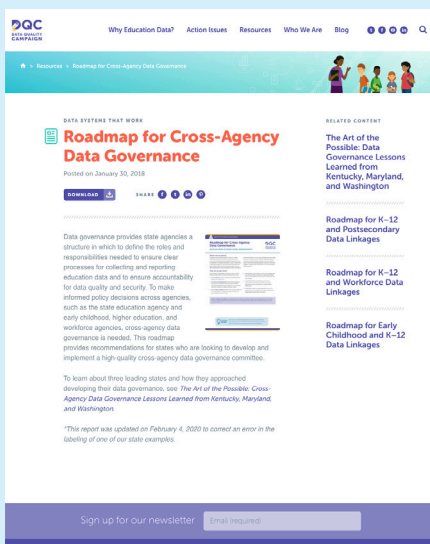
Why Is Data Governance Critical for Helping Policymakers Address Their Data Priorities?

Data governance practices are the best way to ensure that decisions about data collection, privacy, and use are made transparently at the leadership level. Data governance enables state leaders to take the following actions:

- Define roles and responsibilities for managing data collections.

- Make informed policy decisions across agencies.

- Build relationships and trust with stakeholders working on programs spanning from early education through the workforce.

- Create sustainability for data policies and priorities.

See DQC's *Roadmap for Cross-Agency Data Governance* for more information about creating a high-quality data governance body.
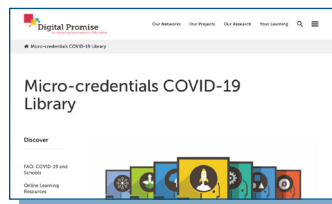
Resources

States can refer to the resources below for clear, actionable information related to safeguarding student data during COVID-19 response and recovery.
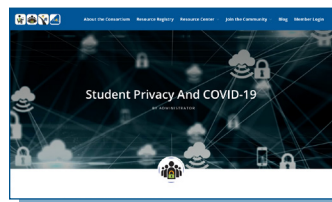
Best Practices for the Design and Implementation of Data Privacy and Security Programs, an issue brief from the Institute of Education Sciences, details best practices for developing and implementing privacy and security plans and data sharing agreements for statewide agencies.
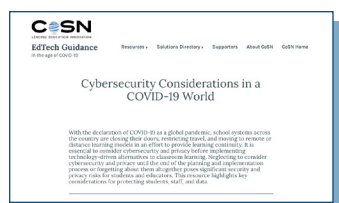
"COPPA Guidance for Ed Tech Companies and Schools during the Coronavirus," from the US Federal Trade Commission, contains advice for schools that use education technology services, including a checklist of considerations for vendor selection.

"Cybersecurity Considerations in a COVID-19 World," released by the Consortium for School Networking, is a rundown of best practices for leaders to consider to ensure that practitioners can protect student and staff data during this shift to online learning.

"FERPA and Virtual Learning," created by the US Department of Education's Student Privacy Policy Office, includes curated resources related to the Federal Educational Rights and Privacy Act (FERPA) and virtual learning for COVID-19 response, including an FAQ to help school officials protect student privacy.

"Micro-credentials COVID-19 Library," created by Digital Promise, helps teachers and administrators continue their professional development. The library includes training modules on data literacy, student data privacy, and technology coaching.
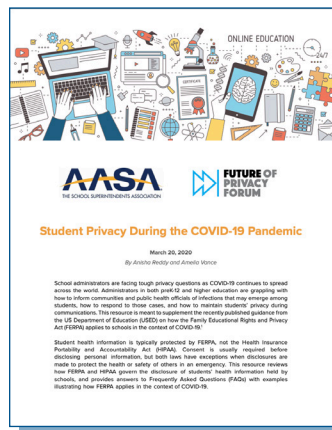
"Student Privacy and COVID-19" is a resource page from the Student Data Privacy Consortium that features tools, including a vendor registry and contract models, to help state agencies and districts manage online learning needs while respecting student privacy.

Student Privacy During the COVID-19 Pandemic, an FAQ from AASA, The School Superintendents Association and the Future of Privacy Forum, offers guidance for school administrators that builds on the guidance issued by the US Department of Education.

The Data Quality Campaign is a nonprofit policy and advocacy organization leading the effort to bring every part of the education community together to empower educators, families, and policymakers with quality information to make decisions that ensure that students excel. For more information, go to www.dataqualitycampaign.org and follow us on Facebook and Twitter (@EdDataCampaign).