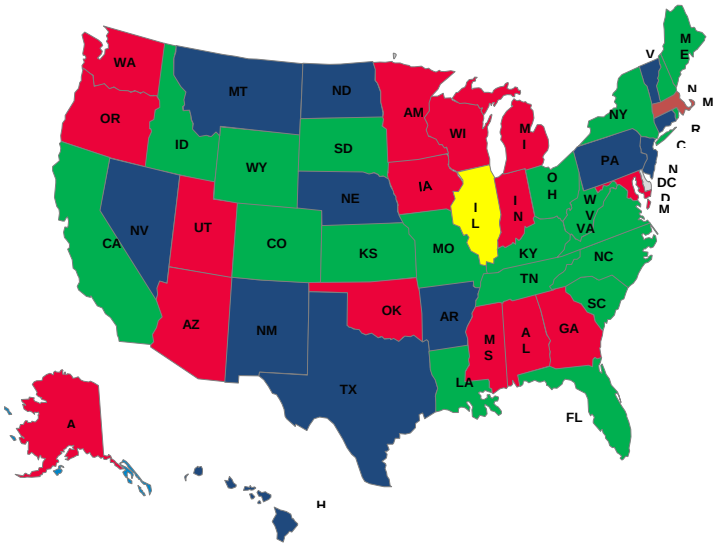
STUDENT DATA PRIVACY: BUILDING A TRUSTED ENVIRONMENT

The effective use of student data is essential for improving student outcomes and equipping educators with the information they need to help every student remain on a path to educational success. Student data can help teachers personalize and customize instruction, equip parents and students with information to make informed educational choices, and assist policymakers with program evaluations and resource allocations. In a world where knowledge is power, student data provides parents, students, and educators with the tools they need to ensure every student attains his or her potential.

At the same time, parents and students must be able to trust that student educational data is secure, kept private, and used solely for the betterment of students' educational experience. Recent legislative activity indicates the ongoing policy questions regarding how student data is collected, stored, used, and shared.

In 2014, 37 different states introduced a total of 110 student data privacy bills, and 28 of those bills ultimately passed into law in 20 states.

- All student data bills failed
- Passed at least one student data bill
- No student data bills in 2014
- At least one student data bill pending



In a world where knowledge is power, student data provides parents, students, and educators with the tools they need to ensure every student attains his or her potential.

WHAT PRINCIPLES SHOULD GUIDE STUDENT DATA PRIVACY POLICIES?

1. **Value of Data**: Student educational data is crucial for improving student outcomes and fostering an environment of personalized learning that will benefit every student.
2. **Openness**: Schools should communicate clearly with parents about how student data is collected, stored, used and shared.
3. **Limited Collection:** Schools should not collect any information beyond what is necessary for student learning and student success.
4. **Limited Use**: Students and parents need to trust that student data is protected and used solely for the purpose of improving student learning.
5. **Accurate and Accessible:** Schools must ensure that student data is accurate, up to date, and readily available to parents and students.
6. **Security**: Schools and SEAs should clarify who is responsible for ensuring student data is protected and secure, and implement policies, systems, and procedures as necessary to ensure security.
7. **Accountability**: Schools and SEAs should conduct compliance audits, perform related oversight, and provide remedies to parents for privacy or security breaches or other misuse of student data.

ExcelinEd's Recommended Student Data Privacy Policies

- **Inventory what type of data is being collected.** Knowing what information is collected is the first step towards protecting it. States should perform regular audits and publish an inventory of what student data is currently being collected. Any data proposed for future collection should have a supporting statement explaining why such is necessary to improve student outcomes.
- **Avoid unnecessary collection.** Schools should not collect any information that is unnecessary for student learning, such as political affiliation, voting history or religion.
- **Ensure data remains close to the student.** Multiple layers of data should exist to ensure there are adequate protections around the flow of student data, detailing what can be collected at the school, and how much of that information is permitted to flow to the district, to the state, and lastly, the federal government. For example, while there would be benefits for school personnel to know certain medical information on students, such as if a student has an allergy or requires the administering of medicine, such information need not go beyond the school's doors. This is true for other governmental entities as well as private companies and nonprofits providing services to a school through an online gradebook, an online course, a dual enrollment program, or a personalized, blended learning platform.
- **Define parental access.** Parents should have the explicit right to access and review their child's education record. Schools should provide electronic copies of student records to their parents upon request. Schools should also regularly (at least annually) notify parents of their rights as they relate to their child's personal information.
- **Establish a Chief Privacy Officer**. States should create the position of a Chief Privacy Officer for education at the state level. This individual would be charged as the primary person responsible for ensuring all educational privacy and security policies—federal and state—are faithfully implemented. The CPO would work with the legislature, the Department of Education, local districts, and the general public to share best practices and develop policies to foster a culture that respects privacy and security. Parents need to know to whom they can turn if they feel their child's privacy was violated. Schools need someone they can consult with to guide their practices and procedures. And districts would have access to a new source of support, best practices, and guidance.