Student Data Privacy

Student data is a commodity that the multi-billion-dollar EdTech industry packages, shares, and sells to advertisers, colleges, data aggregators, and anyone else willing to pay. The "data dossiers" that schools or EdTech providers compile are valuable for profiling our children today and targeting them as future customers.

Why Worry?

In the hands of EdTech and those they share it with or sell it to, student data can negatively impact college admissions, employment, access to credit, financial futures, and more.

The massive amount of data collected by EdTech providers is also an attractive target for hackers and other bad actors (as seen with the **2025 breach of Powerschool**). Compromised social security numbers, just one example of a risk, can lead to our children's identities being stolen and their credit scores destroyed, impacting their future ability to get loans, buy homes, and get credit cards.

What information is being collected?

- **Personally identifiable information (PII)**
- **Grades**
- **Answers to tests and surveys**
- **Behavioral information**
- **Attendance records**
- **Psychological profiles**
- **Disabilities**

Laws to Protect Student Data

The primary statute for protecting student data is the Family Educational Rights & Privacy Act (FERPA). FERPA was designed in 1974—a time of mimeograph machines and calculators. In short, FERPA is outdated, does not work in our modern digital economy, and is not enforced.

Parents have little ability to prevent EdTech from accessing student data. FERPA's "school official exception" lets schools disclose student data without parental consent, as long as the school maintains "direct control" over the provider (which could be as basic as the school agreeing to a provider's boilerplate Terms of Service).

Parents cannot sue schools under FERPA because it grants the U.S. Department of Education exclusive oversight of schools' compliance with FERPA. Parents also face serious hurdles suing EdTech providers because schools, not parents, own the contractual relationship. State privacy laws generally exempt data covered by FERPA.

Action Sheet 8

Take Action!

Student Data Privacy

What Can We Do to Protect Student Data?

WORK WITH YOUR SCHOOL

- Ask your principal and district leadership about opting out of ALL EdTech products or NON-CORE products (such as YouTube). Many schools have a form for this.
- Ask for books and paper-based assignments. Less screen time lowers privacy risks.

WORK WITH DISTRICT LEADERSHIP

- Take your concerns to the Board of Education; most allow public comments at meetings.
- Lobby to use only EdTech that commits to not sharing student data (or using it for advertising or analytics short retention periods, and deletion of all student data at the end of the year.

WORK WITH THE TECHNOLOGY DEPARTMENT

- Ask to register your child on Apps used in school with an alias or anonymous account.
- Advocate to reduce the number of EdTech products used by your school to just a handful so that your school can truly perform the oversight necessary to protect student data.
- Ask for regular audits of EdTech providers, and for the results of those to be publicly posted.
- Insist that schools incorporate contract provisions that preclude sharing and selling of student data, and that all contracts be posted publicly.
- Request that all student data be deleted by EdTech annually.

WORK WITH OTHER PARENTS

- Band together with others: create a committee that meets regularly, logs concerns, and shares them with the Chief Technology Officer, the Superintendent, and the General Counsel.
- Lobby your federal legislators to amend and update FERPA, and to compel the U.S. Department of Education to begin enforcing FERPA with regard to EdTech access to student data.
- Contact the Federal Trade Commission (FTC) or your State Attorney General when you believe EdTech violated its privacy promises. These organizations have different tools for addressing concerns outside of FERPA.