

# Protecting Student Privacy in a Trusted Learning Environment

*Privacy continues to be a primary concern for school districts.*

By Keith R. Krueger



**P**rivacy is often a contentious issue that raises deeply held fears. Concerns about privacy have been rising in the United States since the revelations of the National Security Agency's electronic monitoring, the theft of Target customers' credit card data, and the shuttering of student data platform inBloom.

Privacy debates are often divisive, putting superintendents and other educators on the defensive. Parents believe that too much data are collected about their children, and that those data are left unsecured and are used inappropriately by companies for commercial gain.

Trust is at the heart of this privacy debate. According to author Stephen Covey, "Trust is the glue of life. It's the most essential ingredient in effective communication. It's the foundational principle that holds all relationships."

## Shared Guidance

The best example of the evolving context around the privacy of student data is a recently released set of student privacy principles (<http://studentdataprinciples.org/>).

Last fall, the Consortium for School Networking (CoSN) and the Data Quality Campaign convened representatives from diverse national education groups to reach a consensus on how student data should best be handled and protected. Their audacious goal was to create a set of common guiding beliefs from the education community.

Thirty-eight of the most prominent education non-profits have endorsed the principles since the effort went public in March, including ASBO International and professional associations representing school boards, state education officials, teachers' unions, and the National

PTA. The “10 Foundational Principles for Using and Safeguarding Students’ Personal Information” are grounded in the following statements:

- High-quality education data are essential for improving students’ achievement and preparing them for success in life.
- Data can empower educators, students, and families to make decisions to help all learners succeed.
- Everyone who uses student information has a responsibility to maintain students’ privacy and the security of their data.
- That responsibility starts with limiting the data that are collected, stored, shared, and used to support student learning and success.
- Whenever possible, aggregated data that do not identify individual students should be used to inform key policy decisions and to help improve services and systems that benefit students.

## Desperate Measures

For some time now, education leaders have been saying that we need to move beyond compliance toward aspirational practices. The student data principles do just that.

## It’s too easy to shrug off the concerns as “conspiracy theories” run amok, but they are often genuine.

Although policymakers at the federal and state levels continue to pursue legislation intended to codify into law a wide variety of privacy protections, the education technology community has worked intensely to comply with existing laws, to understand the growing privacy concerns, and to identify aspirational practices in K–12 education.

This issue of trust is critical to keep in mind as education leaders talk with parents and school staff about privacy. It’s too easy to shrug off the concerns as “conspiracy theories” run amok, but they are often genuine. And with parents feeling increasingly as though they have lost control over much of their lives, it is understandable that they are trying desperately to protect the personal identity of their children.

A wealth of new resources on privacy compliance and other smart practices are included in a free CoSN tool kit, “Protecting Privacy in Connected Learning” ([www.cosn.org/focus-areas/leadership-vision/protecting-privacy](http://www.cosn.org/focus-areas/leadership-vision/protecting-privacy)). Also, K–12 online service providers have taken a significant step by signing the Student Privacy Pledge developed by the Future of Privacy Forum and the Software and Information Industry Association. Nearly 150 of the most prominent education technology companies have signed the industry pledge, which was endorsed by President Obama.

So how can you create more trust in your community? Define what those new aspirational principles look like at the school and district level. Be more transparent in your communications about why schools need data and how to protect that data. CoSN is working toward those goals with its new Trusted Learning Environment (TLE) Seal initiative.

## The Trust Imperative

As privacy continues to be a concern for school systems, keeping student data private and secure becomes more difficult. Given the serious repercussions that are possible with data breaches, students and parents want assurances from school system leaders that their data privacy is being protected. To date, no tangible way exists to be sure of that protection. CoSN’s unique, exciting effort calls for the creation of a voluntary, aspirational TLE Seal that goes beyond legal compliance. The TLE Seal intends to represent a learning environment in which students can take advantage of the newest technologies while having their data secure and private.

The first step is to define what those aspirational practices look like at the school and district levels. CoSN—along with its three leading partners AASA, ASBO, and ASCD and a network of 28 school districts—has created a draft set of aspirational practices that identifies a trusted learning environment. Although the aforementioned Student Privacy Pledge has created a marketplace norm with regard to the collection and handling of student data, no such norm exists for school systems. For the first time, the TLE Seal will provide school system leaders with a way of communicating their privacy practices to parents and other stakeholders and the assurance that the school district is adhering to best practices regarding student data privacy. The TLE Seal will be available to all K–12 school systems.

The TLE project will also provide schools with the necessary tools to help them communicate why schools need data and how those data are protected. CoSN will work with key national educational organizations and will align with related efforts in K–12 education to disseminate the work so that the TLE Seal will become the symbol of a trusted learning environment.

The official launch is expected to be at the CoSN Annual Conference in Washington, D.C., April 4–7, 2016. In the meantime, please visit CoSN’s website ([www.cosn.org](http://www.cosn.org)) for the most up-to-date information. Join the trust conversation today!

---

**Keith Krueger** is CEO of the Consortium for School Networking in Washington, D.C. Email: [keith@cosn.org](mailto:keith@cosn.org); Twitter: @keithkrueger

Contributing to this column were **Bob Moore**, chief technology officer of the Dallas Independent School District in Texas, and **Marci Giang**, project manager at CoSN.