A DISTRICT GUIDE TO

DATA MINIMIZATION IN THE AGE OF AI

PIPC

AASA

INTRODUCTION

"For K-12 schools, cyber incidents are so prevalent that, on average, there is more than one incident per school day."

– Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security

The recent Powerschool breach sent shockwaves through the education community, exposing the sensitive information of more than 60 million students and 10 million teachers. Unfortunately, the Powerschool breach is not an isolated incident. The Texas Attorney General's lawsuit against PowerSchool shows this isn't just about data breaches anymore—it's about legal accountability for protecting our students' futures. Unfortunately, the PowerSchool breach is not an isolated incident. Student data is under constant attack.

The urgency of this issue has intensified with the AI revolution. As our companion article "AI Changes Everything: Why Student Data Review Can't Wait Another Semester" details, sophisticated AI models don't just steal data—they connect it across datasets in ways that make even seemingly harmless information dangerous. AI can transform today's attendance records or learning analytics into tomorrow's identity theft schemes. This risk multiplies exponentially as AI models continue to become more sophisticated and grow in their capacity to find connections across datasets. This makes our traditional approach to student data inadequate for the AI era we've already entered.

Now is the perfect time to ensure your school's data policies align with your commitment to student privacy and protecting the children you serve. The AI revolution has compressed our timeline for action—what might have been a multi-year privacy initiative must now happen this school year.

Here's how to get started.

DATA THAT ISN'T COLLECTED CANNOT BE BREACHED.

How should schools navigate deciding what information to collect? Over-collection significantly increases the risk for student information to be exploited for identity theft and fraud, especially as AI systems become more capable of linking disparate data sources. However, schools must collect specific data to function effectively and provide students with better educational services. Not collecting enough data risks non-compliance with reporting requirements and potentially missing opportunities to better serve students.

This balance has become increasingly challenging for schools. Evolving guidance around program eligibility has left many districts uncertain about whether they should collect additional categories of student data at enrollment. The proliferation of edtech platforms and data analytics tools enables schools to collect more granular information about students than ever before—from learning patterns and behavioral data to detailed demographic profiles.

The solution lies in a fundamental shift toward data minimization in education. Schools must collect only the information that is truly necessary, using it only for its intended educational purpose, and retaining only what you need for as long as you need it, before securely destroying it.

This resource will help you systematically review your current data practices, identify quick wins for improvement, and implement a data minimization framework that protects students for years to come without compromising your educational mission.

Data Minimization Framework

The most effective way to begin implementing data minimization is through a systematic review of your current information collection and retention practices. Use these three key questions to evaluate every piece of information your school collects.

1. What student data does your school collect?

Pay attention to what data your school is collecting throughout the school year. Schools may be surprised by how much information they're collecting once they map it out completely.

Schools may collect data across:

- **Enrollment Forms:** What information do families provide during registration?
- **Program Applications:** What additional data do you collect for free and reduced price lunch, special education, gifted programs, or other services?
- **Technology Platforms:** What information do educational apps, learning management systems, and student information systems collect and store?
- **Extracurricular Activities:** What data do you gather for sports, clubs, or field trips?
- **Health and Safety:** What medical, emergency contact, or behavioral information do you maintain?
- **Safety and Discipline:** What surveillance, discipline, or behavioral information do you collect and maintain?

Pro tip: Start by identifying what information your school will collect in standard back-to-school paperwork such as enrollment forms, program applications, and packets sent home to families. Ask school staff across various roles to take a few minutes to compile and print out the various forms and data collection tools they use, sharing it with a point person who is looking into this or bringing them to a district leadership team meeting for discussion.

2. Why does your school collect this information?

For each piece of data you identified, ask yourself:

- **Is this information *necessary* to achieve your specific purpose?** Just because you've always collected certain information doesn't mean it's required. For example, imagine your school collects student fingerprints or palm scans to speed up lunch lines and help prevent delays from younger students forgetting their PIN numbers. Does the school really *need* to collect biometric data to do this? The answer is no; the school has a variety of other ways to simplify the lunch line process, including scanning barcodes on student ID cards or even simply having staff verify student names.

- **Is there a *less invasive* way to achieve that purpose?** Look for alternatives that accomplish the same goal with less personal information. Continuing with our previous example, biometric identifiers are an extremely sensitive category of personal information that can pose significant privacy risks if they are misused or exposed in a data breach, especially since they may be kept beyond a student's time at school. Replacing biometrics with student ID card barcodes or name verification procedures would be much less invasive–*and less risky*–to students.

If you can't clearly articulate why your school needs a specific type of information and how it directly supports your educational mission, you probably shouldn't be collecting it.

3. How long does your school retain this information?

Generally, shorter retention periods reduce risk exposure and storage costs. However, once a school decides to record information — *such as by entering data into Student Information Systems (SIS) or adding to students' education records* — data retention laws may require schools to retain it for years. For example, Virginia's retention schedule sets different retention requirements depending on the type of data, such as:

- 0 Years after end of academic year: student essays and projects;
- 1 Year after end of academic year: report cards and for Career and Technical Education (CTE) enrollment records;
- 5 Years after end of academic year: teacher's grade books and reports for classes associated with graduation requirements;
- 5 Years after student graduates, completes Board of Education program, transfers, or withdraws: cumulative health records and for English as a Second Language (ESL) records; and
- 7 Years after student graduates, completes Board of Education program, transfers, or withdraws: records of a student who has participated in special education programs and separated from the school district post-June 30, 2024.

Ask Yourself: Does your school need to retain this information at all?

Don't assume you need to hold on to everything. Explore whether your school can adopt a policy of reviewing documentation to confirm program eligibility without retaining the underlying information within those documents.

For example, imagine that your school receives a grant that requires the school to verify that all students enrolled in a particular program are within a specific age range. Here's an example of how your school could do this in a more privacy-protective way:

1. Parents bring original legal documents listing the child's age (such as showing their birthdate) to the program enrollment office.
2. A designated staff member reviews the document in person, checking that:
    - The child's name matches the enrollment forms;
    - The date of birth establishes age eligibility for the program; and
    - The document appears authentic.
3. The staff member completes a simple verification log entry, containing:
    - Date of review: [DATE]
    - Student name: [NAME]
    - Document type reviewed: (ex., Birth Certificate)
    - Eligibility confirmed: Yes/No
    - Reviewed by: [STAFF INITIALS]
4. The original document is immediately returned to the parent, and
5. The verification log becomes part of the student's education record, which is subject to privacy protections in the Family Educational Rights and Privacy Act (FERPA).

The school has now confirmed eligibility without retaining copies of legal documents that contain unnecessary sensitive information, which could be breached, lost, or misused.

But what about FERPA?

In general, the Family Educational Rights and Privacy Act (FERPA) does **not** set retention schedules for any student data that schools collect. However, **FERPA has one critical rule related to record retention**: if a parent or eligible student requests access to their personally identifiable information (PII) in education records, the school cannot delete that information while the request is pending

Implementation Roadmap

Now that you've completed your data minimization review, it's time to put your findings into action. Focus on quick wins first to immediately reduce your risk exposure, then build sustainable systems for ongoing privacy protection moving forward.

QUICK WINS FOR THIS SCHOOL YEAR

THESE CHANGES CAN BE IMPLEMENTED QUICKLY FOR IMMEDIATE PRIVACY IMPROVEMENTS.

1. Update enrollment forms and program applications to remove unnecessary information fields.

Review your back-to-school paperwork with fresh eyes. Remove any fields that didn't pass your minimization test, which may include information such as:

- Social Security Numbers (SSNs);
- Biometric identifiers;
- Family financial information beyond what's needed for program eligibility;
- Demographic questions that aren't required for state reporting; and
- Emergency contact information beyond what's reasonably necessary.

ACTIONABLE STEP: REVISE FORMS TO MITIGATE THE RISKS OF OVER-COLLECTING STUDENT DATA DURING THE NEXT ENROLLMENT PERIOD.

SSNs and other identity-related documents are particularly sensitive information commonly sought after by hackers because they can be easily used to facilitate identity theft. This is especially critical for children whose compromised data may not surface as identity theft until years later — imagine a third-grader whose SSN is stolen today facing financial fraud when applying for college loans. Schools should be especially cognizant of when they choose to collect and retain this information, keeping in mind that such collection may make them a more desirable target for hackers and other cybercriminals.

Several states already have laws regulating schools' collection and use of SSNs. For example:

- Virginia prohibits the Department of Education and school boards from requiring students or their parents to provide the student's SSN, instead issuing unique student identification numbers that do not include or derive from student SSNs (§ 22.1-287.03. Unique student identification numbers.);

- If requesting SSNs, Maine requires schools to inform parents and students over 18 what purpose the SSN will be used for and provide them an opportunity to opt out of providing the SSN (§6001-C. Student social security numbers; collection and deletion);

- If the Department of Education or school district's Board of Education discloses the statutory authority for collecting SSNs and how they will be used, Oklahoma allows schools to collect SSNs "for the Department to administer any provision of the Oklahoma School Testing Program Act, for the collection of appropriate and necessary data pursuant to the Oklahoma Educational Indicators Program, for the purpose of determining student enrollment, to establish a mobility rate or for the allocation of State Aid Formula and midyear adjustment in funding for student growth." The law prohibits schools from denying students "any right, benefit, or privilege provided by law" because of their refusal to disclose SSNs (§74-3111. Use of Social Security numbers by state or subdivision prohibited - Exceptions.); and

- West Virginia requires student SSNs or a nine-digit alternative assigned by the county board to enroll in public school. While schools can use SSNs for internal record keeping purposes or studies, the law prohibits schools from displaying SSNs to identify students in certain circumstances (§18-2-5f. Use of student social security numbers).

2. Clearly differentiate between what data collection is required and what is optional

Many families or students provide information simply because it's on a form, not because it's actually required. Make this distinction crystal clear:

- Mark all required fields with asterisks, bold text, a highlight, or different colored text;
- Add explanatory language like "Required for enrollment" or "Optional—helps us serve your child better by" and add a high-level explanation.
- Separate required enrollment information from optional/supplementary details; and
- Consider using separate forms to collect required and optional information.

ACTIONABLE STEP: REVIEW ALL FAMILY-FACING FORMS AND CLEARLY LABEL WHAT'S REQUIRED VERSUS OPTIONAL BEFORE THE NEXT ENROLLMENT PERIOD.

3. Train front office staff on the limitations of data collection.

Your front office team often makes split-second decisions about what information to request from families during the enrollment process. Ensure they understand:

- The information legally required for enrollment, not just what may be helpful;
- Best practices for communicating with families about educational data uses and student privacy protections;
- How to respond to common student privacy-related questions that frequently come up at the start of the school year; and
- Where to direct parents for additional information on the school's student privacy practices.

ACTIONABLE STEP: SCHEDULE A BRIEF TRAINING SESSION BEFORE SCHOOL STARTS TO REVIEW THE ENROLLMENT PROCESS, CHANGES TO ENROLLMENT REQUIREMENTS, COMMON STUDENT PRIVACY SCENARIOS RELATED TO ENROLLMENT, AND STUDENT PRIVACY COMMUNICATION STRATEGIES.

For more information on effective student privacy communications strategies, see the *Student Privacy Communications Toolkit: For Schools & Districts* (Future of Privacy Forum).

Ongoing Policy Development

Minor, consistent improvements in your school's privacy practices will have a much greater impact than attempting to overhaul everything at once. Start with your quick wins (above) and then build momentum for longer-term changes.

1. Create clear data retention schedules and procedures.

Ensure your school has written policies that specify how long different types of information should be kept. These policies should:

- Align retention periods with state requirements and practical needs;
- Identify procedures for securely destroying data when retention periods expire;
- Require training on proper disposal methods for both physical and digital records; and
- Document retention decisions to demonstrate compliance with your policies.

GOAL: LIMIT THE AMOUNT OF STUDENT DATA THAT MAY BE COMPROMISED AND USED TO THE DETRIMENT OF STUDENTS IN THE EVENT OF A DATA BREACH BY DESTROYING STUDENT DATA THAT IS NO LONGER NEEDED.

2. Build privacy considerations into technology procurement.

Many schools discover that they're sharing more student data with vendors than is necessary. Going forward, make privacy protection a standard part of your technology decision-making:

- Create a spreadsheet listing each technology used in your school, who the vendor is, what data you are sharing with them, and whether that sharing is truly necessary for the service provided;
- Limit student data sharing to only what information is necessary for the vendor to provide the contracted service, and (if applicable) require the vendor to delete unnecessary categories of student data they may have previously collected;
- Review existing and future vendor contracts to ensure the school can audit vendor practices and terminate agreements if privacy standards aren't met; and
- Require vendors to securely destroy student data upon the school's request or upon termination of the agreement, whichever comes first.

See our *K-12 Privacy Policy Guide: How to Quickly Spot Red Flags* as a first step to quickly find big problems in privacy policies that would likely restrict the tool from being used with students.

GOAL: DEVELOP A STANDARDIZED PROCUREMENT PROCESS TO THOROUGHLY VET TECHNOLOGIES FOR PRIVACY AND SECURITY SAFEGUARDS *BEFORE* THEY ARE USED IN YOUR SCHOOL.

3. Foster a culture of privacy within your school.

Privacy protection isn't a one-time project—it requires ongoing attention as your programs and technology evolve. To foster a culture of privacy within your school:

- Assign responsibility for privacy oversight to a specific staff member or team;
- Train all staff with access to student information on federal and state student privacy legal requirements and best practices;
- Implement security best practices, such as role-based access controls, to limit which individuals can access student information;
- Create a simple reporting mechanism for staff to flag potential privacy concerns; and
- Schedule annual reviews of your school's data collection practices, as well as a time to revisit data retention schedules and ensure they are being followed.

GOAL: BUILD INTERNAL CAPACITY AND SET UP PROCESSES TO ENSURE STUDENT PRIVACY IS PROTECTED FOR YEARS TO COME.

*Special thanks to Michael Klein for their substantial contributions to the creation of this resource.