SECTION VII.
Student privacy FAQs

Here are some answers to commonly asked questions about student privacy. We urge parents to consult the entire toolkit for more information. If you can't find what you're looking for, email us at info@studentprivacymatters.org. We'll do our best to find answers to your questions!

Q: What is FERPA and what records does it protect?

A: The Federal Education Rights and Privacy Act (FERPA) was enacted in 1974 to protect the privacy of "education records" of students in schools and universities that receive federal funds. Education records are defined as those that are "(1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution." For more information, see Section II.

Q: Under what circumstances can the contents of my child's education record be shared without parental consent?

A: FERPA has been relaxed through regulation in recent years, allowing schools to disclose personal information in your child's education record to third parties under a variety of conditions. For an explanation of these circumstances, see Section II.

Q: Can my child's personal information be shared with every employee within the school?

A: No. A student's personal information can be shared only with those members of the school staff directly responsible for his or her education or services, and only as much information as necessary for them to fulfill their professional duties.

Q: Can my school or district share my child's information with the state education department without parental consent?

A. Yes. Most schools and/or districts report student-level information with the state department of education on a regular basis; some of this data may be required to meet accountability provisions outlined in federal or state law. Other data collection may be purely discretionary on the part of the state. Student information sent by schools to the state is typically stored in the statewide longitudinal data system (SLDS) and may be linked with data from other state agencies, including health and human services, higher education, labor, corrections, and public safety. Information held in the SLDS may then be made available to researchers and policymakers if the state decides to do so. Nearly every state in the nation has an SLDS; the goal of the SLDS program is to track students from preschool through high school, college, and beyond.

WHAT STUDENT DATA IS IN YOUR STATE'S SLDS?

Every state in the nation, except Wyoming, New Mexico, and Alabama, received federal grant funding from the U.S. Department of Education to develop or maintain an SLDS. States that received funds were required to adopt the following minimum requirements for their data systems:

1. A unique identifier for every student that does not permit a student to be individually identified (except as permitted by federal and state law);
2. The school enrollment history, demographic characteristics, and program participation record of every student;
3. Information on when a student enrolls, transfers, drops out, or graduates from a school;

4. Students' scores on state tests as required by the Elementary and Secondary Education Act;
5. Information on students who are not tested, by grade and subject;
6. Students' scores on tests measuring whether they're ready for college;
7. A way to identify teachers and to match teachers to their students;
8. Information from students' transcripts, specifically courses taken and grades earned;
9. Data on students' success in college, including whether they enrolled in remedial courses;
10. Data on whether K-12 students are prepared to succeed in college;
11. A system of auditing data for quality, validity, and reliability; and
12. The ability to share data from preschool through postsecondary education data systems.

NOTE: Many state SLDS contain information specifically identifying students including names, addresses, disability diagnoses, and even suspension details.

Find out how much federal grant funding your state received to develop or maintain a statewide longitudinal data system (SLDS) at http://bit.ly/SPTK_SLDS [1] and learn details about your state's SLDS at http://www.workforcedqc.org/state-solutions

Q: Can I access information in my child's education record? What should I do if it is inaccurate?

A: Yes. FERPA guarantees parents the opportunity to inspect and review your child's education records within 45 days upon request, whether they are held by the school, the district, or the state. You cannot be charged a fee for the school or education agency to search or retrieve these records, but a minimum fee may be charged to make copies. FERPA also gives you the right to correct information in your child's records if you believe it is "inaccurate, misleading, or in violation of the privacy rights of the student." For more information about your rights to access and correct or challenge information in an education record, see Section II.

Q: Is my child's medical information included in her/his education record? Is it protected by HIPAA (the Health Insurance Portability and Accountability Act)?

A: In most cases, medical information that you or your child provides to the school, as well as records made by a school nurse, counselor, or school-operated health clinic, become part of the education record and are covered by FERPA, not HIPAA. The disability and support services that a special education student receives are also part of their education record, and can be disclosed without parental consent under the conditions or exceptions noted in Section II.

Generally speaking, schools are not required to comply with HIPAA because they are not considered "covered entities" under the law, such as health plans, health care clearinghouses, and health care providers. Regardless, you should ask your school who has access to your child's medical, disability or counseling records, and advocate for this information to be closely held within the school and for its disclosure outside the school to be limited as much as possible. To learn more about HIPAA in schools, please visit http://bit.ly/SPTK_HIPAA [2]

Q: If I email my child's teacher about a confidential issue, will that information be included in my child's education record?

A: It could be. If you have a sensitive matter you want to discuss with your child's teacher, we suggest scheduling a private face-to-face meeting to discuss your concerns. Anything written that you share—handwritten notes or email communication—could become part of your child's education record.

Q: Is my child's digital information collected by classroom applications (apps) or online programs protected by FERPA?

A: It depends on many factors including, but not limited to, what student information the classroom app or online program collects and/or maintains, and how it uses and shares the information. FERPA became law in 1974, long before technology became so pervasive in our classrooms. While the U.S. Department of Education Privacy Technical Assistance Center (PTAC) has attempted to provide some guidance on this issue, schools and districts are advised to evaluate on a "case-by case basis" whether FERPA applies. Until federal law is updated and strengthened to protect all student information—digital or otherwise—we offer important recommendations you can share with your school, district, and/or state in Section IV.

Q: My child's teacher or principal told me a classroom app or online program used in my school is FERPA compliant. What does this mean?

A: This statement should not reassure you that your child's information is kept private or is well-protected. FERPA allows for broad disclosures of personal information contained in student records without parental consent, as described in Section II, and the law requires no minimum standards for data security protections. Additionally, FERPA regulates the practices of schools that receive federal funds; it does not directly regulate the actions of private vendors or online operators. If a vendor or operator uses student information for an unauthorized purpose, parents should hold local education officials accountable to maintain strict oversight and stop the practice. For more information on best practices, please refer to Section IV.

Q: What is the punishment for a FERPA violation?

A. If a school is found in violation of FERPA, federal funding may be withheld. However, the federal government has never done this in FERPA's 43-year history. Additionally, certain third parties may be banned by the U.S. Department of Education from receiving student's personal information for up to five years if the party re-disclosed student data in violation of FERPA. If an organization fails to destroy student information after it's no longer needed for purposes of a "study," it may also be banned from receiving student information for up to five years.

Q: Is my child's teacher allowed by law to sign up my child for classroom apps or online programs without my permission?

A: Under the "school official" exception, FERPA allows your teacher to use personal information from your child's education record to create an online account without your consent. This may also be done with a more limited set of student information using the "directory information" exception. However, if your child is under the age of 13 and is entering personal information into a child-directed online program himself, either at school or at home, the federal Children's Online Privacy Protection Act (COPPA) would apply. A teacher may consent to your child's use of an online educational tool if any personal information collected by the online vendor or operator is not used for any commercial purpose. It is the responsibility of the school, district, or state to ensure that the vendor or operator uses student information only for specified purposes and secures it sufficiently. As noted in Section IV, we recommend that no teacher should sign up students to online programs without a careful vetting of the program at the school, district, or state level.

MORE INFORMATION ON COPPA IN SCHOOLS

For a teacher/school to provide consent on behalf of a parent, the operator of the classroom app or online program must provide the school with all the notices required under COPPA.

Additionally, upon request by the school, the operator must provide the school:

1. A description of the types of personal information collected on students;
2. An opportunity to review the student's personal information and/or have the information deleted; and
3. The opportunity to prevent further use or online collection of a child's personal information.

For more information about parent's rights under COPPA, see Section II.

Q: Can personal student information be sold by schools or the companies they allow to collect it? Can it be used to target advertisements to students?

A: Many state laws, including California's 2014 landmark Student Online Personal Information Protection Act (SOPIPA), prohibit companies that collect data through their online educational services from selling student information — except when a vendor or operator's company is acquired by another company, in which case the new vendor or operator must comply with all privacy provisions in the law. SOPIPA and some other state laws also prohibit the use of personal student data for targeted advertising.[3]

FERPA prohibits companies designated as "school officials" from using student data for any reason other than the purpose originally authorized, unless a parent or eligible student has provided consent for an additional purpose. That is, unless the school has authorized a company to use student data for targeted ads, supposedly for educational purposes, or the parent or eligible student consents, the company may not do so. However, FERPA does allow the disclosure of "directory information" without limitations, including marketing to students and selling the information to others. For more on directory information and how to opt out of its disclosure, see Section II.

COPPA prevents vendors or operators of child-directed websites or apps from using personal information that is collected directly from a student under the age of 13 for commercial purposes, such as marketing or sharing the information with other companies for that purpose, unless a parent provides consent.

The Protection of Pupil Rights Amendment (PPRA) requires schools to notify parents and allow them to opt-out when students are "scheduled to participate in activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes, or to sell or otherwise provide that information to others for marketing purposes." However, PPRA does allow companies, vendors, and operators to use students' personal information for the "exclusive purpose of developing, evaluating, or providing educational products or services for students or schools."

Q: Do companies offering college entrance exams, e.g., the College Board (PSAT/SAT) and ACT, sell information my child provides voluntarily?

A: Yes. You may have noticed a check box as part of the PSAT, SAT or ACT online registration form asking you or your child to opt in to sharing his or her information with colleges and scholarship programs. On each exam day, your child may also be encouraged to check the same box and provide more information. If you or your child opt in, your child's personal profile may then be sold to eligible colleges or other organizations for marketing or admissions decisions. To protect your child's privacy, we recommend that no extraneous personal information be provided to the College Board or ACT by either you or your child.

NOTE: If you've already opted-in to sharing your child's information through the College Board (SAT) Student Search Service, it is possible to revoke your permission by visiting: https://student.collegeboard.org/student-search-service/opt-out

Q: My child told me she/he took a survey at school which asked very personal questions. Is this allowed?

A: Under the PPRA, written parental consent must be obtained before a child can be asked to take a federally-funded survey, analysis, or evaluation that asks questions related to political affiliations, religious beliefs, sexual behavior and attitudes, and other sensitive

issues. If the survey asks questions about these types of personal issues but is not federally funded, parents must be notified in advance and be allowed to opt their children out of taking the survey. For more on PPRA and the type of questions it regulates see Section II.

Q: Does the school have an obligation to inform parents when there is a breach of student data?

A: None of the federal student privacy laws (FERPA, COPPA, PPRA) require schools to inform parents when student information has been breached. However, some state laws require this notification. In addition, FERPA requires that schools maintain in your child's education record an additional record of any unauthorized disclosures such as a data breach, and must make that information available to parents upon request. For more information, see Section II. As incidents of data breach in education are on the rise, we urge parents to advocate for stronger breach disclosure rules at the school, district, and state levels.

Q: Is it true that military recruiters can obtain my high school child's personal information directly from the school? Can I refuse to allow the school to provide it?

A: Yes. Under Section 9528 of No Child Left Behind (NCLB) and under Section 8025 of the Every Student Succeeds Act (ESSA), military recruiters may request access to the contact information of students. Parents can opt out of this disclosure by submitting a written refusal form to the school or district; see Appendix C for a sample form.

Q: What are "data walls," and under what circumstances are they prohibited?

A: Data walls are charts that teachers use to display students' test scores and/or progress in a subject or skill. FERPA generally prohibits the disclosure of such personal student information to non-school officials without the consent of the parent. If the information on a data wall includes your child's name or other identifying information, such as student ID, along with grades or test scores, is visible to any non-school employee in a semi-public area such as a classroom or hallway, and was posted without your consent, this violates FERPA.

HOW CAN DATA WALLS CONTRIBUTE TO STEREOTYPING?

Prior to the start of school, teachers may view details from a student's academic file, including grades, attendance, exam scores, and disciplinary records via a data wall or through an online interface called a data dashboard. Students with positive histories may benefit from a phenomenon known as the "Pygmalion effect," whereby teachers will have higher expectations of those students leading to an increase in performance. Students with poor histories may suffer from the "Golem effect," whereby teachers will have lower expectations placed upon them leading to poorer performance.[4]

Q: What should I do if I believe my child's rights have been violated?

A: If you believe that your rights under any federal law have been violated, including FERPA, PPRA, or COPPA, you should notify your school, district Superintendent, and/or school board as soon as possible. If they refuse to take appropriate action, you may contact your local chapter of the American Civil Liberties Union (ACLU) to request help, or file a complaint. For details on how to do so, see Section II.

Need help? Contact the Parent Coalition for Student Privacy at info@studentprivacymatters.org so we can connect you with other supportive groups and/or resources!

Disclaimer: While the goal of the Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood is to provide valuable resources to help you protect student privacy, our suggestions should not be used in place of legal advice from an attorney. For questions on how federal, state, and local laws and policies may apply to your situation, you may wish to seek the advice of a licensed attorney by contacting your local bar association's referral service.

Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

REFERENCES

1. https://nces.ed.gov/programs/slds/stateinfo.asp

2. https://www.hhs.gov/hipaa/for-professionals/faq/513/does-hipaa-apply-to-an-elementary-school/index.html

3. https://fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide_Nov-4-2016.pdf

4. http://www.oxfordbibliographies.com/view/document/obo-9780199846740/obo-9780199846740-0014.xml