SECTION IV.

Student privacy best practices for states, districts, schools, and teachers

In an ideal world, sensitive student information would be held under lock and key and shared only with parental permission to trusted teachers, counselors, tutors, and other school staff. While this may not be possible in today's data- and technology-driven schools, it is important to implement thoughtful best practices to safeguard student information at the state, district, and school level.

These recommendations come from our coalition's Five Principals to Protect Student Privacy,[1] the U.S. Department of Education's Privacy Technical Assistance Center (PTAC),[2] and other expert organizations concerned with this issue. Though our best practices may go beyond what's required in current federal and state law, states, districts, schools and their teachers should implement these policies if they want to improve student privacy and security protections and limit their own liability. Share these with your school today!

THE IMPORTANCE OF WRITTEN AGREEMENTS

One of the best methods to help protect student information is to require written agreements, contracts, or memoranda of understanding (MOUs) between states/schools/districts and any third parties accessing or receiving personal student information, including companies who offer online instructional programs or free classroom applications (apps). Written agreements can limit how student information is collected, used, and shared with others; they can also require the company to adopt strong security and breach notification requirements, include enforceable penalties for noncompliance, and enumerate recourse procedures for parents. For a complete list of what should be included in written agreements, see the Consortium of School Network's (CoSN) document titled "Suggested Contract Terms," (http://bit.ly/SPTK_COSN)[3] and a sample contract prepared by the Massachusetts Student Privacy Alliance (http://bit.ly/SPTK_MSPA).[4]

Note: If states, schools and/or districts share student information with organizations and agencies without parental consent as allowed under the FERPA "studies" or "audit or evaluation" exceptions, as described in Section II, a written agreement is required. See the "Written Agreement Checklist" (http://bit.ly/SPTK_WAC)[5] provided by the U.S. Department of Education Privacy Technical Assistance Center for more information.

Best practices for state education departments

REQUIRE written agreements, contracts, or MOUs between the state and any third parties receiving personal student information, and post them prominently on the state's website.

APPOINT a Chief Privacy Officer who is an expert in the law and privacy and security practices to be responsible for establishing a comprehensive data governance program and communicating with parents who have questions or concerns.

CREATE a data stakeholder advisory council that includes parents, teachers, and privacy experts to provide input and oversee student data collection, governance, and disclosure.

The U. S. Department of Education Privacy Technical Assistance Center recommends that data governance programs should address:
"• protection of sensitive data;
• vulnerability assessment and risk management;
• enforcement of legal, regulatory, contractual, and architectural compliance requirements;
• identification of stakeholders, such as parents and administrators, their roles and responsibilities; and
• access management."

This is critical to ensure that privacy and security are prioritized and that the public has input into decisions pertaining to the use of student personal information.

ASSESS online instructional programs and free classroom apps for their educational content and purpose, data use practices, and privacy and security standards, and approve or reject them accordingly. No online programs or apps should be considered for use from any vendors or operators that have not signed a contract with the state and agreed to the Student Privacy Pledge, [6] which bans the sale of personal student information except in the case of mergers, acquisitions, and bankruptcies. Signers of the Student Privacy Pledge also commit to not using student information "for behavioral targeting of advertisements to students."

Best practices for school districts and schools

REQUIRE written agreements, contracts, or MOUs between the district/school and any third parties accessing or receiving personal student information. Post them prominently on the school or district website and contact parents directly with information about where to read them.

The Consortium of School Networks (CoSN) recommends that contracts should: "Include a specific restriction on the use of student information by the provider for advertising or marketing purposes or the sale or disclosure of student information by providers."[7]

Fordham Law School recommends that "cloud service agreements" should: "Include a clause explicitly addressing the sale and marketing of transferred data or the use of that data by the vendor itself for sale and marketing purposes without parental consent."[8]

ADOPT and adhere to the state education department's approved list of online programs and apps, and post the current list on the district or school website. Districts may also choose to create an even more rigorous procedure for vetting online programs and apps.

DESIGNATE a Chief Privacy Officer or someone on staff responsible for ensuring best practices and communicating with parents.

WORK WITH parents, teachers, and privacy advocates to adopt transparent policies around the collection, use, and protection of student data, including:

- Identifying and then minimizing the collection of personal student information;
- Justifying the purpose for each type of collection, including an explanation of its educational purpose;
- Describing how the information is collected, stored, and protected from breaches, and how parents can access and, if necessary, correct it;
- Identifying to whom the information will be disclosed (including individuals, organizations, or vendors or operators outside the school or district) and for what purposes; and
- Defining the process for notifying parents before information is disclosed.

We recommend that notification to parents should include:
• A list of the classroom apps and online programs students are required or encouraged to use.
• The educational purpose or value of each app or online program.
• Student data that each app or online program will collect.
• Key provisions of each app or online program's privacy policy.
• Whether parents can opt out of their children's use of the apps or online programs, and if so, what alternatives will be provided.
• Whether an app or online program collects and analyzes data to create a learning profile that will direct a student's lessons or educational pathways. If it does, parents should have the technology explained to them and a way to challenge its accuracy and utility.

PROHIBIT schools from disclosing any personal student data, including "directory information," to any third parties who intend to sell or use student information for marketing purposes.

ADOPT a policy allowing parents to specify which "directory information" can be shared and with which third parties. For more information, see Section II.

ASK FOR parent permission or consent before sharing highly sensitive data such as disability, health, and disciplinary data with third parties, including vendors, operators, or other organizations.

■ PROVIDE regular data security training, including best practices, to teachers, administrators, and anyone who handles personal student data.

Fordham Law School recommends: "For larger districts and those with extensive cloud networks and intensive data transfers, the designation of a chief privacy officer with responsibility for data governance, privacy compliance, and teacher training is necessary to assure proper stewardship of student data and to enable those districts to more effectively assure the protection of their students' information."

■ PROHIBIT teachers from assigning or encouraging students to use any classroom apps or online programs not on the state or district approved list.

■ PROHIBIT "data walls" displaying a student's personal information, including names or other identifying information, from being posted in any semi-public areas, including classrooms or hallways.

Best practices for teachers

■ BEFORE ASSIGNING an online program or classroom app, consider whether its use is necessary — many privacy issues can be avoided by simply not adopting every new online tool marketed to schools.

The U. S. Department of Education Privacy Technical Assistance Center recommends that schools and districts "[h]ave policies and procedures to evaluate and approve proposed online educational services."

■ DO NOT USE or ask students to use any online program or app unless it has first been vetted and approved by your state education department or district.

■ BE PREPARED to offer an appropriate alternative (e.g., a textbook or paper and pencil version) to students whose parents choose to opt out of an online program that accesses their personal information.

Houston Independent School District developed a system to evaluate the privacy, safety, and security of commonly used Web Apps. You can check out the criteria used to rate them here: http://www.houstonisd.org/Page/126147

■ NEVER SIGN UP for online programs or classroom apps with "click-wrap" agreements — when a user checks a box to accept terms and conditions before using a product or service — unless the terms have been rigorously reviewed by someone with legal and/or technical expertise. Remember that even with review, the terms of service may change over time, putting students' privacy at risk. To learn more about click-wrap agreements, see PTAC's guidance at http://bit.ly/SPTK_PTAC [9]

■ EDUCATE YOURSELF in the principles of good digital citizenship and incorporate responsible technology practices in your classroom. Incorporate Fordham Law School's "Privacy Educators Classroom" curriculum into your lessons, found at https://www.fordham.edu/info/24071/privacy_education.

Sign up today for privacy trainings offered by the U.S. Department of Education at http://ptac.ed.gov/

■ WHEN CREATING "data walls" that display students' test scores or grades in public areas like classrooms or hallways, never include any information that could be used to identify them.

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. http://www.studentprivacymatters.org/five-principles-to-protect-study-privacy/

2. http://ptac.ed.gov/

3. http://www.cosn.org/sites/default/files/pdf/Suggested_Contract_Terms_09_2014.pdf

4. https://secure2.cpsd.us/mspa/MSPA_Student_Data_Privacy_Agreement_V4.pdf

5. http://ptac.ed.gov/sites/default/files/Written_Agreement_Checklist.pdf

6. https://studentprivacypledge.org/

7. http://cosn.org/sites/default/files/CoSN-Privacy-Toolkit.pdf

8. http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip

9. http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf