SECTION III:
What teachers should know about federal student privacy laws

One way for teachers to protect themselves and their students is to understand their responsibilities under federal law. There are five major federal laws governing the use and disclosure of a student's personal information: **FERPA** (Family Educational Rights and Privacy Act), **NSLA** (National School Lunch Act), **IDEA** (Individuals with Disabilities Education Act), **PPRA** (Protection of Pupil Rights Amendment), and **COPPA** (Children's Online Privacy Protection Act). In each case, we will provide practical examples of how the laws apply to you as an educator.

Additionally, 39 states plus the District of Columbia have passed student privacy-related education laws since 2013. A few of these laws also have specific provisions that protect teacher data. For example, New York passed a law in 2014 prohibiting the disclosure, sale, or use of educator evaluation data for marketing purposes by districts, third-party contractors, or their assignees. In 2017, New Hampshire passed a law preventing teachers from being video recorded during evaluations without written consent of the teacher as well as the parents of each affected student. To learn more about your state's privacy laws, refer to the Parent Coalition for Student Privacy and Network for Public Education's *State Student Privacy Laws: A 50 State Report Card,* to be released in November 2018.

It's important to note that individual school districts may have policies in place that limit the sharing of student information beyond what state and federal law requires. Educators should contact their local boards of education to learn about local policies that may place additional protections for student or teacher privacy.

If you witness or experience what you believe to be privacy violations described in this section, first contact your union and then school administrators, your district, or the state department of education. You can also contact the Privacy Technical Assistance Center of the U.S. Department of Education to ask for advice as to how to proceed, or reach out to the advocacy organizations concerned with student privacy listed in Section VII.

Family Educational Rights and Privacy Act (FERPA)
(20 U.S.C. § 1232g; 34 CFR Part 99)

The Family Educational Rights and Privacy Act (FERPA) became law in 1974 and applies to schools receiving federal funds. Administered by the U.S. Department of Education, FERPA is the broadest federal law regulating student privacy, but in many ways it has been weakened to allow for the increased sharing of personal student data rather than strengthened for the digital age.

FERPA protects personally identifiable information (or PII) contained in student education records. Protected PII includes, but is not limited to, a student's name; the name of the student's parent or relatives; physical address; Social Security number or student ID number; biometric record; date of birth, place of birth, and mother's maiden name; or other information that, alone or in combination, would allow others to identify the student. Education records include, but are not limited to, grades, transcripts, class lists, student course schedules, health information, and student discipline data.

The general rule is that schools and teachers cannot disclose student PII — whether orally, written, or in electronic form — from education records without first obtaining permission from parents. However, the following exceptions have been incorporated into FERPA to allow for data disclosure without parental consent:

"DIRECTORY INFORMATION" *exception:*

Directory information is a limited set of information from students' education records that is not considered highly sensitive or an invasion of privacy if disclosed, including their names, addresses, phone numbers, date and place of birth, participation in school activities and sports, awards and recognitions, and dates of attendance. Schools may disclose students' directory information to third parties without parental consent if public notice has been provided to parents containing the types of information designated as "directory information," a statement of a parent's right to restrict or opt-out of its disclosure, and the period of time in which parents may exercise this right. Directory information is traditionally shared with school photography and yearbook companies, but schools are increasingly using this exception to upload class lists and share other student data to ed tech companies. See Scenario 1 below for more detail.

"SCHOOL OFFICIAL" *exception:*

Schools may disclose student PII from education records without parental consent to other "school officials," including vendors, consultants, contractors, and volunteers with "legitimate educational interests" performing "institutional services or functions" for the school. However, those designated "school officials" must meet certain conditions, including being under the "direct control" of the school, which may require a contract or other written agreement. They must also not use the data for any purpose not authorized. Many school vendors and other contractors often receive and collect student information without parental consent under the "school official" exception. See Scenario 1 for more detail.

"AUDIT AND EVALUATION" *exception:*

Disclosure of student PII in education records is also allowable without parental consent to "authorized representatives" of "Federal, State, and local educational authorities conducting an audit, evaluation, or enforcement of education programs." Under this exception, student data is often disclosed without parental consent to the state department of education and related agencies, or to other "authorized representatives" designated by a district, as long as there is a written agreement restricting the use of the data for that purpose.

"STUDIES" *exception:*

A fourth exception allows disclosures of student PII in education records without parental consent to organizations or individuals for "studies." These studies must be limited to the purpose of "developing, validating, or administering predictive tests; administering student aid programs; or improving instruction." Again, there must be a written agreement restricting the use of the data for this purpose before this disclosure can occur. This exception is generally used when schools disclose student information without parental consent to researchers or testing companies.

Scenario 1

Q: I want to use a free app that allows me to award points to students for good classroom behavior. After creating a teacher account, the app is asking for student names, class periods, and photos. Does FERPA allow me to share this information?

A: First, has your school or district vetted this app for compliance with state or federal privacy law? If not, you must be very careful. Best practice in any case is to obtain district, school, and parental consent before using any app that collects personal student information.

Should you decide not to seek parental consent, FERPA allows schools to disclose a limited set of student data with third parties under the "directory information" exception. If you intend to use this exception, make sure any information you load into the app aligns with the types of information your school or district designates as directory information. See above for more details. You should also verify whether any parents have opted-out of disclosure of their child's directory information. Otherwise, you could be violating FERPA.

The "school official" exception may also apply in this case but only if the app meets certain criteria. First, the app must have a "legitimate educational interest," perform an "institutional service or function" on behalf of the school, and be under the school's "direct control." Check with your school or district to make sure the app is meeting each of these conditions. It's important to note, however, that the U.S. Department of Education suggests that a good method to determine whether the app company is under the school's direct control is to read the Terms of Service (TOS). For example, if the app provider claims it may change the terms at any time without notice to you, the user, this may violate FERPA.

If the TOS allows for personal data to be used for non-educational or commercial purposes, this may also violate FERPA. Finally, if your students are under the age of 13 and will be entering personal information themselves into the online app, additional restrictions may apply. For more information, see the Children's Online Privacy Protection Act (COPPA) section on page 18.

Scenario 2

Q: My school uses a "data wall" to group students by assessment scores or academic progress. It's posted in a main hallway of the school. Does this violate FERPA?

A: If a data wall is visible to the public, and information displayed includes student names or other information that could identify them, along with their test scores or grades or other personal information from their education records, the data wall is likely in violation of FERPA. If you must use data walls, remove any identifying student information and/or ensure they are located in a private space such as the principal's office. For more reasons why data walls may do more harm than good, see relevant articles listed in the Resources section.

Scenario 3

Q: Our administration sends out a weekly newsletter to the entire school staff with announcements and other important information. One section names students who have been suspended and the reason for the suspension. Is this in violation of FERPA?

A: Yes! Personally identifiable information or PII contained in a student's education record, including disciplinary information, should be made available only to those school staff members who are directly involved in a child's education. This applies also to school staff who may be able

to view this information through student databases or information systems, such as Infinite Campus or PowerSchool. Only school employees with a "need to know" should be provided access to personal information in the student's education records, including digital data.

Individuals with Disabilities Education Act (IDEA)

(Public Law No. 94-142)

The Individuals with Disabilities Education Act (IDEA) is designed to protect the rights of children with disabilities, including students with Individualized Education Programs or IEPs, who are to be provided with a free and appropriate education.

The law is administered by the U.S. Department of Education and gives parents the right to consent before their child's PII can be disclosed in the following circumstances: 1) to participating agencies providing or paying for transition services used to facilitate a child's movement from school to after-school activities; 2) when a public-school child with disabilities intends to enroll in a private school in a different district from the parents' residence; and 3) each year before the district can disclose special education service records for reimbursement from the federal government.

Scenario 4

Q: A parent requested that all information relating to her child's Individualized Education Program (IEP), including updates and progress reports, be sent to her via email. Does IDEA allow this?

A: Parents may receive email copies of their child's IEP and progress reports if:

1) the school obtains prior parental consent;
2) the parents provide their confidential email address;
3) a secure password is used to access documents;
4) hard copies are provided upon request; and
5) parents may refuse the email option at any time.

National School Lunch Act (NSLA)

(79 P.L. 396, 60 Stat. 230)

The National School Lunch Act (NSLA) became law in 1946 and is administered by the U.S. Department of Agriculture (USDA). It protects confidential information collected by schools used to determine whether a child is eligible to receive free or reduced-priced lunch (FRL) or free milk under the National School Lunch Program.

In general, NSLA requires prior parental consent before FRL eligibility information, including household size and family income, can be shared with parties inside or outside of the school. Only school officials directly responsible for the child's education should be allowed access to eligibility status (whether they are eligible for free meals or free milk or reduced-price meals), and schools must make efforts to prevent "overt identification" of a child's FRL status.

Scenario 5

Q: Students receiving FRL at my school are given color-coded lunch tickets, and their purchases are tracked on a paper spreadsheet posted next to the cafeteria register. Does NSLA allow this?

A: No. NSLA prohibits "overt identification" of students' FRL status. Schools must make efforts to mask or otherwise de-identify a student's eligibility status to prevent others — especially other students — from viewing or accessing it. To prevent overt identification, schools should be sure not to publicize eligible families' or children's names. Schools should not have have separate dining areas, service times, or serving lines, or use any other method including colored meal cards, tickets, or tokens that could be used to differentiate students receiving free or subsidized meals.

Protection of Pupil Rights Amendment (PPRA)

(20 U.S.C. § 1232h; 34 CFR Part 98)

The Protection of Pupil Rights Amendment (PPRA), enacted in 1978, is administered by the U.S. Department of Education. PPRA requires schools to provide direct notice to parents of the right to refuse their child's participation in certain activities, at least annually at the beginning of the school year, and when the following activities may occur:

"MARKETING SURVEYS:"

Marketing surveys involving collection, disclosure, or use of personal information obtained from students for marketing purposes or to sell or "otherwise distribute the information" to others.

"EXAMS AND SCREENINGS:"

Non-emergency, invasive physical exams or screenings of students administered by the school, which are unnecessary to protect the immediate health and safety of a student, except for hearing, vision, or scoliosis screenings.

"SURVEYS, ANALYSES, AND EVALUATIONS:"

Surveys, analyses, and evaluations administered to students that are not federally funded and concern any of the following eight sensitive areas:

- Political affiliations or beliefs of the student or the student's parent;
- Mental and psychological problems of the student or the student's family;
- Religious affiliations and beliefs;
- Sex behavior and attitudes;
- Illegal, anti-social, self-incriminating, and demeaning behavior;
- Critical appraisals of close family members;
- Legally recognized privileged relationships, such as those of lawyers, physicians, and ministers; or
- Income (other than that required by law to determine eligibility for a program).

If any survey, analysis, or evaluation that deals with issues listed above is funded in whole or in part by a program of the U.S. Department of Education, parents must provide prior consent before their children are given these surveys.

Additionally, parents have the right to inspect the content of any surveys described previously, as well as any "instructional content that is provided to a student, regardless of its format, including printed or representational materials, audio-visual materials, and materials in electronic or digital formats (such as materials accessible through the Internet). The term does not include academic tests or academic assessments."

Scenario 6

Q: My school's counseling department intends to administer a survey to students about their drug and alcohol use. Does PPRA allow this?

A: Before administering a student survey that asks questions related to any of the sensitive areas listed on the previous page, schools must provide parents direct notice of when the survey will occur and an opportunity to view it and opt-out of their children's participation. If the survey is funded by a program of the U.S. Department of Education, parents must give prior consent. In general, schools should make every effort to ensure students' answers to surveys of any kind are confidential. Electronic surveys requiring students to log in with their name or student number are not considered anonymous. Survey tools like Google Forms or SurveyMonkey may provide some anonymity, but only if the privacy settings are utilized correctly.

Scenario 7

Q: Our state recently adopted the College Board's SAT college entrance exam as the mandatory annual state standardized test. On test day, students are instructed to complete a pre-exam survey asking questions about their religious affiliation and parental income. Is this allowed?

A: Historically, students taking college entrance exams did so voluntarily, and they registered and paid for the test themselves or with their parents' assistance. More recently, states and school districts are administering the PSAT, SAT, or ACT to all eligible students during the school day. In this case, schools pay for the exam and register students with the testing companies on their behalf.

The U.S. Department of Education's Privacy Technical Assistance Center recently issued guidance instructing states and school districts administering college entrance tests in this manner to notify parents and obtain their written consent before asking students questions that relate to religion, income, or other sensitive information covered under PPRA. Schools must also obtain prior written parental consent if student PII, including test scores, test score ranges, or demographic information is disclosed by the testing companies to third parties. Failure to do so can result in a violation of FERPA and IDEA. For a link to the Department's important guidance documents, see the Resources section.

Children's Online Privacy Protection Act (COPPA)

(15 U.S.C. 6501-6505)

The Children's Online Privacy Protection Act (COPPA) was enacted by Congress in 1998 and is enforced by the Federal Trade Commission (FTC).

COPPA regulates the activity of "operators" of child-directed websites, including education-related online programs or applications that collect, use, or disclose personal information collected online directly from children under the

age of 13. In general, COPPA requires operators to obtain parental consent prior to collecting children's personal information from them — including a child's name, email, phone number, screen name, geolocation, photo, voice recording, or other persistent unique identifier — and provide clear and prominent use of its data disclosure practices on its website.

Yet the FTC allows schools and teachers to act as a parent's agent and provide consent on their behalf — but only where the operator collects student's personal information for the use and sole benefit of the school and for no other commercial purpose.

When schools or teachers consent on behalf of parents, the FTC requires operators to provide the school notice of disclosure practices, as mentioned above, and the right for the school to request that the operator delete students' personal information and cease further collection or use.

Scenario 8

Q: My elementary school has a 1:1 program where each student is provided her/his own laptop. Teachers are encouraged to find education-related apps and load them directly to the devices. When I find one I like, I create a teacher account, agree to the app's Terms of Service (TOS), and assign my students to use the program, which then collects their personal data. Does this violate COPPA?

A: As explained in Scenario 1, your school or district should be vetting any technology that collects personal student information, including programs with "click-wrap" agreements where the user merely checks a box agreeing to the TOS before using an app. Whether or not your school or district has evaluated the product for compliance with federal and state privacy laws, best practice is to first obtain parental consent.

If you intend to provide parental consent on behalf of your students' parents, COPPA requires that the operator of the online program collecting their personal information uses it solely for the benefit of the school and not for any commercial purposes. The only way to know how an operator intends to use students' information is to read the TOS and Privacy Policy, which are typically long, confusing, full of jargon, and sometimes contradictory. COPPA doesn't provide a definition of "commercial purposes" and the FTC's guidance on this issue is limited, so it's up to schools and teachers to interpret whether they can act on a parent's behalf to provide consent.