



UNITED STATES DEPARTMENT OF EDUCATION

STUDENT PRIVACY POLICY OFFICE

October 26, 2022

Dear Chief State School Officers and Superintendents:

The Student Privacy Policy Office (SPPO) at the U.S. Department of Education (Department) provides annual notification to State educational agencies (SEAs) and local educational agencies (LEAs) regarding the educational agencies' obligations under the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) and the Protection of Pupil Rights Amendment (PPRA) (20 U.S.C. § 1232h; 34 CFR Part 98). The annual notification, which is required by 20 U.S.C. § 1232h(c)(5)(C), has not substantively changed since it was last issued. The notification may be accessed via our website at <https://studentprivacy.ed.gov/annual-notice>.

FERPA and PPRA

FERPA is a Federal law that protects the privacy rights of parents and students regarding education records maintained by educational agencies and institutions that receive funds under a program administered by the Department. FERPA covers education records maintained by such entities, as well as education records maintained by other parties, such as third-party technology vendors, to whom the agency or institution has outsourced institutional services or functions. PPRA affords parents and students with rights concerning certain SEA and LEA marketing activities, the administration or distribution of certain surveys to students, the administration of certain physical examinations or screenings to students, and parental access to certain instructional materials. Resources on FERPA and PPRA, including SPPO's online FERPA training modules, our technical assistance request process, and our complaint process, can be accessed on our website at <https://studentprivacy.ed.gov/>. We also recommend that you sign up for our monthly student privacy newsletter by visiting <https://studentprivacy.ed.gov/subscribe-student-privacy-newsletter>.

SPPO Resources

In addition to those referenced above, the following specific resources may also be helpful.

- *FERPA and Virtual Learning Resources* – identifies resources that may be helpful in supporting virtual learning.
<https://studentprivacy.ed.gov/resources/ferpa-and-virtual-learning>
- *PPRA General Guidance* – provides plain-language guidance on PPRA for parents and students.
<https://studentprivacy.ed.gov/resources/protection-pupil-rights-amendment-ppra-general-guidance>

- *A Parent's Guide to FERPA* – provides plain-language guidance on FERPA for parents and eligible students.
<https://studentprivacy.ed.gov/resources/ferpa-general-guidance-parents>
- Videos: *FERPA's Complaint Process Explained* and *What Happens When I File A Complaint?* – provide a succinct overview of the SPPO complaint process.
<https://studentprivacy.ed.gov/file-a-complaint>
- Video: *What is the Protection of Pupil Rights Amendment or PPRA?* – provides a succinct description of PPRA.
<https://studentprivacy.ed.gov/training/what-protection-pupil-rights-amendment>

Transparency Best Practices

SPPO is near the completion of a five-year study of a nationally representative sample of websites from LEAs, identifying whether and how these websites include information about student privacy. The final report is scheduled for release this fall. Although not specifically required by FERPA or PPRA, SPPO encourages LEAs to post on their websites their FERPA and PPRA notices and policies to improve the transparency of information on student privacy. The combined results from the first three-quarters of the sample, reported in October 2021, show that only about half of LEAs reviewed post on their websites the LEA's Annual Notice or directory information notice under FERPA (55 percent and 52 percent, respectively). Less than one-third of LEAs posted on their website the LEA's policies under PPRA (29 percent).

As SEAs and LEAs continue to leverage technology in classrooms, we encourage as much transparency as possible with the school community about the use of such technology, the personally identifiable information from education records you share with online service providers, and the providers' responsibilities regarding that information. The study's October 2021 results found that only 22 percent of LEA websites reviewed have a list of approved online services or apps used in the classroom. For more information about transparency best practices and to review the annual report summaries, please refer to SPPO's LEA website privacy review at <https://studentprivacy.ed.gov/lea-website-privacy-review>.

Data Security Best Practices

Finally, we recognize the growing number of LEAs affected by data breaches, cyber incidents, and ransomware attacks. If an LEA is affected by such incidents, we strongly encourage you to work with the relevant law enforcement and regulatory entities to respond in an appropriate and timely manner. In addition, we encourage you to take advantage of the resources and best practices available on SPPO's website:

- *Data Breach Response Training Kits* – provides customizable exercises designed around a series of scenarios to use for in-house trainings and data breach response exercises.
<https://studentprivacy.ed.gov/resources/data-breach-response-training-kit>
- *A Parent's Guide for Understanding K-12 School Data Breaches* – provides parents of K-12 students information to help understand what a data breach means and provides

tools and best practices to help navigate the sometimes confusing process of protecting children's data in the event of a breach.

<https://studentprivacy.ed.gov/resources/parent%E2%80%99s-guide-understanding-k-12-school-data-breaches>.

Thank you for the important work you do on a daily basis to protect student privacy and provide a safe and effective learning environment for students across the country. The Department is available to assist you with your questions about FERPA, PPRA, and student privacy. You may contact us by submitting your questions to our student privacy help desk at FERPA@ed.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "Kevin Herms".

Kevin Herms
Director
Student Privacy Policy Office