Commercial Companies and FERPA's School Official Exception: A Survey of Privacy Policies

COVID-19 and Edtech Platforms

COVID-19 has presented obstacles to in-person learning, with many schools opting to use education technology ("edtech") platforms as a solution. However, concerns about student privacy have emerged, including those related to commercial companies entering the education sector. To meet the requirements of the Family Educational Rights and Privacy Act ("FERPA"),[1] some consumer-facing vendors have established different privacy policies for their education platforms, setting stricter limits on advertising, for example, than for their commercial platforms. Despite these efforts, challenges in meeting FERPA's requirements may still exist.

FERPA's School Official Exception

FERPA restricts the disclosure of personally identifiable information ("PII") from education records, including disclosure to edtech platforms.[2] Many schools disclose PII to edtech platforms under FERPA's "school official exception," which allows a platform to receive PII from education records without parental consent if it: (1) "performs an institutional service or function," (2) has "a legitimate educational interest" in the education records, (3) "is under the direct control" of the school "with respect to the use and maintenance of education records," and (4) uses education records only for authorized purposes and does not redisclose PII from education records to other parties without consent.[3]

Potential Challenges in Meeting Requirements of the School Official Exception

Despite schools' reliance on the "school official exception" to share student data with edtech companies, the platforms' privacy policies may not meet the exception's requirements. Four common provisions show the challenges:

1.) **Non-consensual deletion of data:** To satisfy the school official exception's requirement of direct control, schools must be able to direct a platform's retention and deletion of student data.[4] However, some privacy policies provide that the vendor may delete content provided by the school at any time without notice to the school. In some cases, deletion may be permitted only if the school violates the provisions of the agreement. If policies permit the deletion of PII from education records without notice to the school or its consent, schools may not be in "direct control" of the data as required for the school official exception to apply.

2.) **Unilateral policy changes:** To comply with the school official exception's requirement of direct control, schools should approve or be notified of changes to privacy policies or contractual terms.[5] However, a privacy policy might provide that student users' personal information will remain subject to the policy unless it is changed by a successor entity. Similarly, other policies provide that a vendor might not give notice of changes if it launches a new service or if the changes are to

provide new functionality in an existing service. If a vendor or its successor is able to unilaterally change policies, it may be difficult for schools to demonstrate direct control of the PII.

3.) **Flow of information between services:** The school official exception requires that data may be used only for the educational purposes authorized by schools. However, one vendor may permit schools to use non-educational services, which may combine personal information from educational services with personal information from other services, including for non-education purposes such as to develop new products. Those non-educational purposes may make the platform ineligible for the school official exception.

4.) **Ambiguous language:** Platforms' policies should be fully transparent to ensure that their data access and use are consistent with the school official exception's limited scope. However, a policy might state that customer data will be used for purposes "compatible" with providing the service, without further clarification to inform students and their families of potential data use. When such language is used, school officials should seek to clarify those terms.

State Regulations on Student Privacy

In addition to FERPA, schools and edtech platforms must comply with state student privacy laws. These laws can include additional restrictions on the deletion of educational data,[6] specify the inclusion of certain contract provisions,[7] and impose additional penalties for violations.[8]

Recommendations

School officials should require the privacy policies of technology vendors to:

- Ensure that schools directly control the deletion of PII from education records.
- Require that platforms obtain schools' consent to, or provide notice of, changes.
- Set strict boundaries between education and commercial uses of student data.
- Be explicit and avoid ambiguous language in explaining how data is used.
- Adhere to the additional requirements that may be imposed by state law.

This two-pager is one of a series designed to give practitioners clear, actionable guidance on how to most responsibly use technology in support of students. Find out more at cdt.org/student-privacy.

Endnotes

1. Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g; 34 C.F.R. Part 99.
2. 34 C.F.R. § 99.30.
3. 34 C.F.R. § 99.31(a)(1).
4. U.S. Dept. of Ed., Protecting Student Privacy While Using Online Educational Services: Model Terms of Service; U.S. Dept. of Ed., Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices.
5. U.S. Dept. of Ed., Responsibilities of Third-Party Service Providers under FERPA at 4.
6. Texas, Tex. Educ. Code § 32.156; Georgia, O.C.G.A. § 20-2-666.
7. Louisiana, La. R.S. § 17:3914; Illinois, 105 ILCS 85/15.
8. Utah, Utah Code § 53E-9-310; New York, N.Y. Educ. Law § 2-d.