FUTURE OF PRIVACY FORUM
fpf.org | October 2018

Sharing Data with Ed Tech: Student Privacy 101 For Higher Education

By Sara Collins, Trevor Schmitt, and Amelia Vance

Overview

The **Family Educational Rights and Privacy Act (FERPA)** is a federal law enacted in 1974 that governs information in a student's education record. The law guarantees that "eligible students" have access to their "education records" and restricts who else can access and use students' "personally identifiable information" (PII). FERPA allows educational institutions to share student data with third-party service providers in certain circumstances. Additionally, many states have requirements beyond FERPA's provisions. This document provides describes best practices for the contracting and use of services from ed tech companies in higher education.

FERPA applies to schools that receive funding from the U.S. Department of Education; virtually all post-secondary institutions (both public and private) receive funding from the Department of Education and are subject to FERPA.

When can student PII be shared with an ed tech company?

A school may share PII with "school officials" without obtaining student consent. A school official is any person or company performing a task that would normally be performed by the school. An ed tech company typically qualifies as a "school official" as long as the company:

1. Performs a service for the school that the school would otherwise perform itself;
2. Falls within the school's annual FERPA notification's provisions for sharing PII without student consent;
3. Allows the school to retain "**direct control**" over the maintenance and use of student data; and
4. Uses the student data only for the purpose for which it was shared and does not further disclose the data without the school's consent.

Although these requirements may seem relatively simple, creating and requiring effective contract terms can be a challenging process.

Gijs utilizes his iPad and MacBook Pro in math class by THINK Global School (thinkglobalschool), Flickr, CC BY-NC-ND 2.0

What is direct control?

While not specifically defined in FERPA, "direct control" has been interpreted to mean that schools maintain full control and decision-making authority over the student data. The school must be able to ensure the company will only collect, use, and share information at the school's direction, or as part of the purpose for which the school contracted with the company in the first place. Schools must also ensure that they can comply with FERPA access requests from students for some or all of the contents of their education record held by an ed tech company. Direct control can be achieved through contractual provisions between schools and companies.

What qualifies as a contract between an ed tech company and a school under FERPA?

Many agreements qualify. Although most people think of contracts as formal documents, use of virtually every web -based tool, mobile app, piece of computer software, and data service involves some sort of agreement. This includes End User License Agreements (EULAs), Terms of Service (TOS), and Click-Through agreements regardless of whether the software or app is free or purchased. Even setting up an account with a digital service often qualifies as an agreement or contract. Because contracts are legally binding, educational institutions who enter into agreements that involve student PII should take care to ensure that they adhere to FERPA standards and that student information will be properly handled, protected, and used.

If a technology does not comply with FERPA requirements, a school cannot direct students to "consent" to data sharing as a workaround. The Department of Education recently issued guidance on this topic, explaining to schools and ed tech companies that schools retain the responsibility of ensuring any mandatory ed tech product is used only in compliance with FERPA protections.

What should be included in the contract?

Contract terms are important. Although each educational institution may use its own contract template or terms, several essential student data focused features should be present in agreements between schools and service providers. Here are a few important best practices:

1. **Clearly define terms.** Definitions are key to determining what specific student data a contract covers. Avoid provisions that narrowly define important terms like "data," "student information," or "personally identifiable" because such definitions may leave certain types of sensitive student data unprotected.

2. **Require notice, or consent, for any changes in the Terms of Service.** Educational institutions are required to maintain control over the student data shared with service providers. Allowing service providers to materially change their TOS without notice or consent likely violates FERPA's requirements.

3. **Be clear about who is responsible for compliance.** Many service provider contracts contain language assigning all legal responsibilities to the educational institution. But from a legal standpoint, service providers may not shift compliance responsibilities to schools. Contracts should not include language to the contrary.

4. **Maintain control over any subsequent data sharing.** Just like educational institutions, service providers often use subcontractors to perform certain data-oriented tasks. All FERPA-related contract provisions should apply to these subcontractors as well.

5. **Require student data to be collected, used, shared, and destroyed responsibly.** Clearly state what data should be collected, how it should be used, when it may be shared, and when it should be destroyed.

6. **Define a strong, flexible security standard.** Failure to protect student PII with adequate security leaves student information vulnerable. Language that requires security in accordance with industry best practice will evolve as better security practices develop.

7. **Determine how student data may be accessed and, if necessary, corrected.** FERPA provides students with the right to access and to correct their data. This right extends indirectly to service providers and contracts should define how service providers will give access to schools who receive such student requests.

8. **Ensure ownership and rights over student data remain with the school.** Contracts should clearly state that the school retains all rights and ownership interest in the student data shared with the service provider.

9. **Explicitly prohibit the software provider from building any personal student profiles other than to support the authorized purpose of the contract.** Allowing service providers to collect or use data to build individual student profiles outside of the purpose of the contract may lead to FERPA violations. This does not mean that the service provider cannot use student data to maintain or improve their service or use de-identified data to show the effectiveness of their service.

10. **Require protection of student data if control of the service provider changes hands.** In the event of a merger, acquisition, or other sale of the service provider, the terms agreed to by the school and the original provider must follow the data, regardless of whether a new entity assumes control of the information.