

## Federal Regulations Related to Artificial Intelligence

The United States does not have a comprehensive law that covers data privacy; instead, there are federal and state laws that cover various types of data privacy, such as financial data or health information. As of 2024, only California and Virginia have enacted comprehensive state privacy laws.

In recent years, two major federal legislative proposals—the American Privacy Rights Act and the American Data Privacy and Protection Act—surfaced, both aiming in different ways to address data privacy, algorithm transparency, and other concerns in a comprehensive manner. While these proposals are not likely to pass any time soon, it is encouraging to see substantive, high-quality policy proposals circulating.

Related to the data privacy of students, there are currently two federal laws worth mentioning.

### 1. The Family Educational Rights and Privacy Act of 1974 (FERPA)

FERPA is the federal law that protects the privacy of student education records and applies to all schools and education agencies that receive funds under an applicable program of the U.S. Department of Education.

The last regulatory updates to FERPA predate the widespread use of technology in learning environments, including the storage of education records, the technological generation of records, and the use of technology to support and assess students. School districts and education institutions that are subject to FERPA must interpret this law for how data is accessed, used, and stored in light of artificial intelligence. For instance, using a program to detect AI usage may require students' work to be processed through an outside third party, which may be a violation of FERPA.

*In 2023, UC Santa Cruz issued guidance and warned that using services that purport to detect when AI is used in assignments should not be used without disclosure and consent required under FERPA unless certain preconditions were undertaken pertaining to the service having been purchased and vetted by the institution or that the tool is “protected from external access.”<sup>1</sup>*

Some of the key components of FERPA as it relates to schools include the following:

- Parents and guardians have rights to access, review, and request amendments to their child's education records until the student turns 18 or enters post-secondary education.
- Schools must obtain written consent before disclosing personally identifiable information (PII), with certain exceptions (e.g., health/safety emergencies, transfers, legal requirements).
- Education records include items like grades, disciplinary records, and transcripts, while directory information (e.g., name, grade level) can be shared unless parents and guardians opt out.
- Educators and schools must protect student data, including when using digital tools and educational apps, ensuring vendors comply with FERPA rules.

---

<sup>1</sup> “Letter to Faculty About Plagiarism Detection Tools,” UC Santa Cruz, 2023, [https://ucsc-expghost.imodules.com/controls/email\\_marketing/view\\_in\\_browser.aspx?sid=1069&gid=1001&sendId=4255642&ecatid=4&puid=](https://ucsc-expghost.imodules.com/controls/email_marketing/view_in_browser.aspx?sid=1069&gid=1001&sendId=4255642&ecatid=4&puid=).

- Annual notifications to parents and guardians are required about their FERPA rights, with the ability to opt out of directory information sharing.

## 2. The Children's Online Privacy Protection Act (COPPA)

COPPA sets specific requirements for operators of websites or online services that knowingly collect personal data from children under the age of 13. Primarily, it requires direct parental or guardian notification and parental or guardian consent for the collection of these children's personal information and allows parents and guardians to control what happens to this data. It establishes that companies that collect this information must have clear policies for what information is collected and how it is secured.

COPPA aims to safeguard young students' personal information from being collected and used without parental or guardian consent, thereby enhancing their online privacy and safety.

Schools often use various online educational tools and platforms. In certain situations, schools can provide consent on behalf of parents and guardians for the collection of students' personal information, particularly when the data is used solely for educational purposes. This places a responsibility on educators and administrators to ensure that the digital tools they employ comply with COPPA regulations and adequately protect student data.

In January 2025, the Federal Trade Commission (FTC) finalized amendments to the COPPA rule to address evolving digital practices and enhance children's online privacy protections. Key updates include:<sup>2</sup>

- **Separate Parental or Guardian Consent for Data Disclosure:** Operators are now required to obtain distinct verifiable parental or guardian consent before disclosing a child's personal information to third parties. This change aims to give parents and guardians more control over their children's data, especially concerning targeted advertising practices.
- **Data Retention and Deletion Policies:** The amendments mandate that operators retain children's personal information only as long as necessary to fulfill the purpose for which it was collected. They must establish and disclose data retention policies and are prohibited from retaining such information indefinitely.
- **Enhanced Oversight of Safe Harbor Programs:** The FTC introduced stricter requirements for COPPA Safe Harbor programs, including more detailed reporting and public disclosure of member operators. This measure aims to increase transparency and accountability among organizations that self-regulate under COPPA guidelines.

These updates underscore the importance for educators and school administrators to stay informed about COPPA regulations. Ensuring that the educational technologies and online services used within schools comply with these enhanced privacy protections is crucial to safeguard student data effectively.

## Higher Education

Unfortunately, there are few federal regulations that govern AI directly at the higher education level. Unlike at the Pre-K–12 level, where a local or state education agency or school district may issue guidance for AI, in higher education, institutions and systems may vary widely in terms of disparate

---

<sup>2</sup> <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data>

policy. While there may be a few examples of university system offices issuing guidance, for the most part, AI guidance is issued by individual institutions or, in many cases, can vary even from department to department within one school.

At the higher education level, a greater degree of academic freedom and autonomy is given to faculty to decide what is taught and how. Attempts at restricting course content or methods could be seen as violating academic freedom. Since most students at higher education institutions are legally adults, there is also a greater degree of control and autonomy given to the student in terms of their own data.

With that said, there are some federal laws that would still apply at the higher education level, including the following:

- The Family Educational Rights and Privacy Act (FERPA) still applies at the higher education level. Students 18 years and older, are required to consent the disclosure of education records. AI tools that use education records and related personally identifiable information must have the consent of students under FERPA.
- Disclosure of medical “treatment records,” including mental health records, are governed under FERPA.
- Laws that prevent bias and discrimination, like Title IX and Title VI of the Civil Rights Act, should guide the creation, use, and applications of AI products to minimize bias and ensure that it does not lead to discrimination against protected classes.

### **Intellectual Property and Research**

U.S. Copyright Law, enshrined in Title VII of the U.S. Code guides copyright and ownership of created works, including journal articles, books, and other covered intellectual property.

Recent guidance from the U.S. copyright office maintains that human-created works, like journal articles or books, are governed under Title VII and that “copyright protects the original expression in a work created by a human author.”<sup>3</sup> It further stated, however, that copyright “does not extend to the purely AI-generated material.” The Copyright Office has indicated that guidance on the use of AI data-scraping copyrighted material will be forthcoming.

---

<sup>3</sup> <https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf>