

The Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act is a federal law in the United States that protects the privacy of student education records. It applies to all educational institutions that receive federal funding, which includes schools and colleges. This federal law also gives certain rights to parents or eligible students (who are a minimum 18 years of age or attending a postsecondary institution). This federal law was enacted in 1974 and also applies to any education agency that receives funds under a suitable program of the US Department of Education.

The main purpose of FERPA is to control access to and disclosure of student records. Schools must obtain written consent from a parent or an eligible student under this federal law before releasing any information from the student's educational records like the student's name, address, social security number, grades, attendance records, and other similar information. Non-compliance with The Family Educational Rights and Privacy Act can result in the loss of federal funding for educational institutions. To ensure compliance with these regulations schools take privacy protection seriously and have policies and procedures in place.

To comply with FERPA regulations, organizations should establish policies and procedures that address the privacy and security of student education records. Some key components that those policies and procedures should cover are:

1. Data security- being able to establish protection measures for student records, training employees in data security practices and incident response.
2. Monitoring and Auditing- Implementation of regular monitoring and auditing such as having internal audits periodically and data security assessments.
3. Training and Education

The Family Educational Rights and Privacy Act is not designed for non profit organizations specifically but there are still some benefits. Compliance with FERPA does encourage non profits to implement security measures for the protection of student education records. This helps to protect the privacy of the students and also helps to protect the organization against data breaches and unauthorized access. Some other benefits include:

1. Reputation and Ethical Consideration- Non profit Organizations are entrusted with sensitive information so complying with FERPA guidelines show dedication and commitment to protecting privacy which can also help increase the reputation of that organization
2. Confidence of Parents and Students- Complying with FERPA guidelines assures parents and students that their education records are being handled with care and confidentiality. Non-profit organizations can use FERPA compliance to build trust with parents and students that they are helping, leading to increased participation and engagement in programs or services.
3. Risk Mitigation and Legal Compliance- failing to reach compliance can have legal and financial consequences so making sure to follow regulations of FERPA will help to avoid

legal issues and mitigate the possibility of losing funding or receiving a penalty, protecting the non profit organizations reputation in the process.

<https://studentprivacy.ed.gov/faq/what-ferpa>

<https://studentprivacy.ed.gov/resources/ferpa-general-guidance-students>

<https://studentprivacy.ed.gov/resources/ferpa-general-guidance-parents>

<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

References:

Fenton, H. (2018). Data Breaches: Nonprofits Are Also at Risk. Venable LLP. Retrieved from <https://www.venable.com/insights/publications/2018/10/data-breaches-nonprofits-are-also-at-risk>

Gibson, J. (2018). The Consequences of PCI DSS Non-Compliance. Tripwire. Retrieved from <https://www.tripwire.com/state-of-security/regulatory-compliance/pci/consequences-of-pci-dss-non-compliance/>

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

New York State. (2020). Stop Hacks and Improve Electronic Data Security Act (SHIELD Act). <https://www.nysenate.gov/legislation/laws/GBS/899-AA>

United States Congress. (2002). Federal Information Security Management Act of 2002. <https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf>

PCI Security Standards Council. (2021). PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv321.pdf