Student Data Privacy (FERPA) Compliance Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The landscape of educational technology (EdTech) is evolving rapidly, necessitating a robust and current understanding of student data privacy laws. The Family Educational Rights and Privacy Act (FERPA), often referred to as the Buckley Amendment, is the cornerstone of this protection, ensuring parents and eligible students have the right to inspect, review, and control the disclosure of education records and Personally Identifiable Information (PII). Non-compliance is not merely an administrative oversight; it exposes institutions to legal liability, federal funding withdrawal, and severe reputational damage, particularly in the age of high-profile data breaches and increased public scrutiny. Student Data Privacy (FERPA) Compliance Training Course is designed to empower every staff member from K-12 school officials to postsecondary administrators to act as a data steward, protecting the confidentiality, integrity, and availability of sensitive student information in both physical and digital environments.

This essential course transcends basic legal awareness, offering real-world scenarios and best practices for navigating the complex intersection of federal law, digital citizenship, and modern data management. We delve into contemporary challenges, including the responsible privacy vetting of EdTech vendors, the secure handling of records in remote learning and hybrid models, and the application of FERPA to evolving concepts like directory information and implicit disclosure. By mastering the clear guidelines on data sharing agreements, parental rights, and the necessary procedures for disclosure without consent, participants will solidify their role in building a culture of institutional trust and risk mitigation. Successful completion will equip all participants with the verifiable skills to ensure legal compliance and uphold the ethical commitment to safeguarding every student?ÇÖs fundamental right to privacy.

Programme Curriculum

Student Data Privacy (FERPA) Compliance Training Course

Introduction

The landscape of educational technology (EdTech) is evolving rapidly, necessitating a robust and current understanding of student data privacy laws. The Family Educational Rights and Privacy Act (FERPA), often referred to as the Buckley Amendment, is the cornerstone of this protection, ensuring parents and eligible students have the right to inspect, review, and control the disclosure of education records and Personally Identifiable Information (PII). Non-compliance is not merely an administrative oversight; it exposes institutions to legal liability, federal funding withdrawal, and severe reputational damage, particularly in the age of high-profile data breaches and increased public scrutiny. Student Data Privacy (FERPA) Compliance Training Course is designed to empower every staff member from K-12 school officials to postsecondary administrators to act as a data steward, protecting the confidentiality, integrity, and availability of sensitive student information in both physical and digital environments.

This essential course transcends basic legal awareness, offering real-world scenarios and best practices for navigating the complex intersection of federal law, digital citizenship, and modern data management. We delve into contemporary challenges, including the responsible privacy vetting of EdTech vendors, the secure handling of records in remote learning and hybrid models, and the application of FERPA to evolving concepts like directory information and implicit disclosure. By mastering the clear guidelines on data sharing agreements, parental rights, and the necessary procedures for disclosure without consent, participants will solidify their role in building a culture of institutional trust and risk mitigation. Successful completion will equip all participants with the verifiable skills to ensure legal compliance and uphold the ethical commitment to safeguarding every student?ÇÖs fundamental right to privacy.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Articulate the core provisions of FERPA and its application to all federally funded educational institutions.
2. Differentiate between Personally Identifiable Information (PII) and Directory Information within the context of student records.
3. Identify the specific student and parental rights concerning the inspection, review, and amendment of education records.
4. Apply the legal guidelines for disclosure without consent
5. Evaluate vendor contracts to ensure robust EdTech privacy vetting and data security clauses are in place.
6. Analyze the transfer of rights from parents to eligible students
7. Recognize and avoid practices leading to implicit disclosure of non-directory information, particularly in class lists or public postings.
8. Implement secure protocols for handling and sharing records in remote and hybrid learning environments.
9. Understand the relationship and overlapping concerns between FERPA, COPPA, and state-level data privacy laws.
10. Develop an effective institutional process for managing parental and student requests for record access and amendment within the 45-day requirement.
11. Practice the appropriate response and reporting procedures for a suspected data breach or unauthorized disclosure.

12. Mitigate compliance risks by adhering to best practices for data minimization and the secure disposal of obsolete records.
13. Promote a culture of data stewardship and digital citizenship across all faculty and staff.

Target Audience

1. All K-12 Teachers and School Officials
2. Higher Education (Postsecondary) Faculty and Staff.
3. School/District IT and Network Administrators.
4. Registrars and Admissions Officers.
5. Human Resources (HR) and Compliance Officers.
6. Counselors and Health Services Staff.
7. Third-Party Vendors/Contractors with Access to PII.
8. School/District Leadership.

Course Modules

Module 1: FERPA Fundamentals and Scope

- What the Family Educational Rights and Privacy Act is and its central goal: protecting PII in education records.
- Identifying which institutions and programs are covered due to federal funding.
- Identifying what constitutes an ?Ç£education record?Ç¥ versus personal memory aids.
- Case Study: A teacher uses a personal, unsecure spreadsheet on their desktop to track student grades. Is this an education record? Analysis of how record storage method and access determine FERPA status.
- Understanding the Eligible Student and the transfer of rights upon age 18 or matriculation.

Module 2: Access, Review, and Amendment Rights

- Parent/Eligible Student's right to access records within the 45-day requirement.
- Procedures for receiving, verifying identity, and fulfilling a formal request for records.
- The process for a parent/student to challenge and seek correction of inaccurate or misleading information.
- Case Study: A parent disputes a disciplinary record entry. How must the institution respond, and what are the steps for the formal hearing process? Focus on due process and record modification procedure.
- Maintaining a clear log of all record requests and disclosures.

Module 3: Disclosure with Consent

- Education records cannot be disclosed without written consent from the parent or eligible student.
- What must be included in a consent form.
- Understanding the right to revoke consent and the procedure for ceasing disclosure.
- Case Study: A private scholarship organization requests a student?ÇÖs transcript. The student signs a generic waiver. Is this sufficient for FERPA? Focus on the specificity and scope required for valid written consent.
- Using and storing a standard, legally-compliant consent form template.

Module 4: Disclosure without Consent (Exceptions)

- Defining and managing the Annual Notification and the right to opt-out of disclosure.

- Understanding the criteria for an employee or contractor to be considered a "school official" with a "legitimate educational interest."
- The protocol for non-consensual disclosure to protect the health or safety of the student or others.
- Case Study: A former student's non-custodial parent demands their adult child's transcript. Which exceptions apply, and what is the proper refusal script? Focus on the 'eligible student' status.
- Procedures for responding to subpoenas, court orders, and ex parte orders.

Module 5: EdTech and Vendor Management

- The compliance obligation when using cloud services or educational applications that store PII.
- A checklist for evaluating new vendors on their data security practices, data handling, and compliance with FERPA/COPPA.
- The four-part requirement for a vendor to operate under the "school official" exception.
- Case Study: A teacher signs up for a new, free online quiz platform and uploads their class roster. Has a FERPA violation likely occurred, and what are the immediate steps? Analysis of unauthorized disclosure via unvetted services.
- The principle of only sharing the minimum PII necessary for the service.

Module 6: Digital Data Security and PII Handling

- Best practices for securing education records in digital storage, on school networks, and on personal devices.
- Mandatory protocols for strong passwords, MFA, and role-based access to sensitive data.
- The immediate steps to take upon suspecting or confirming an unauthorized disclosure or system breach.
- Case Study: An employee's work laptop is stolen, containing an unencrypted file with student PII. What are the notification requirements and risk mitigation steps? Focus on prompt incident response and the reporting chain.
- Training on identifying and avoiding common cyber threats that lead to PII exposure.

Module 7: FERPA in Context: K-12 vs. Postsecondary

- The primary role of parental rights until the student becomes "eligible"
- Navigating the complete transfer of rights to the eligible student and the requirement for a FERPA waiver for parents to access records.
- Avoiding the unintentional release of non-directory information.
- Case Study: An academic advisor discusses a student?ÇÖs failing grades over the phone with the student?ÇÖs concerned mother. The student has not signed a waiver. Is this a violation? Focus on the immediate transfer of rights.
- Guidelines for the secure, mandated destruction of old physical and digital education records.

Module 8: Compliance Culture and Institutional Trust

- Each employee's role in establishing a comprehensive compliance program.
- The necessity of continuous training, written policies, and periodic audits
- Understanding the potential penalties from the Department of Education, including loss of federal funding.
- Case Study: A school is audited following a complaint to the DoE. The finding is a lack of documented staff training and inconsistent policies. What is the institutional path to remediation? Focus on the importance of an auditable compliance trail.

- Promoting the responsible use of student data for learning improvement while strictly maintaining privacy.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com