The Ultimate Guide to Compliance in the Education Sector

Section 2-D, FERPA, and more special regulations to follow with educational

White Paper

CRA™
Transform IT
Computer Resources of America

Introduction

Ecommerce merchants and website owners who work with educational institutions are now legally required to follow special regulations according to the jurisdictions they operate in.

These regulations dictate that collecting, using, and disclosing personal information like a child's name, school grades, IP address, and location can have serious risks for those who fail to comply. Consequently, online businesses that target users residing in related areas must also abide by these laws as long as they continue to service customers from these areas.

Unfortunately, businesses sometimes fail to notice such vulnerabilities until the last minute. Compliance with such laws should not be an afterthought but a critical part of the strategy and due process for organizations that intend to serve the market for the long term.

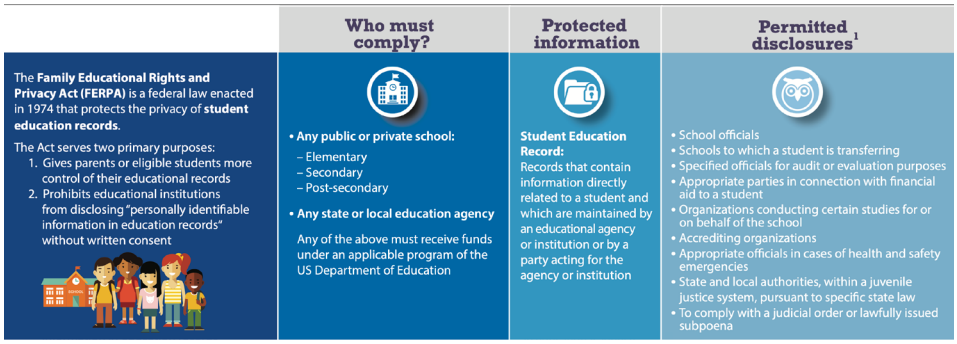
This guide aims to explain some of the critical privacy and information protection laws that affect educational institutions and their partnering organizations.

The Family Educational Rights and Privacy Act (FERPA) Compliance

FERPA defines the privacy standards that protect the personal information of students and their families while giving them the ability to access their records. It applies to any/all educational institutions that are funded from programs administered by the U.S. Department of Education (DOE).

Educational organizations that maintain education records need to give control of these records to their students. Consequently, websites and/or online stores that work with such organizations may be required to comply with FERPA, especially if they also have access to these records. FERPA applies to companies that sell food, textbooks, and other items within the scope of a school.

Companies that work with educational institutions also need to have adequate protective measures in place to protect the personally identifiable information (PII) of their customers.



Source: Public Health Professionals Gateway

Here are nine ways compliance experts believe educational institutions can maintain compliance with FERPA:

Organizations That Come Under FERPA

Given that FERPA applies to any educational institution that receives funding from DOE. These means elementary, secondary, and post-secondary schools, as well as some private and parochial schools, must comply with FERPA.

Information Under FERPA Protection

FERPA protects any/all information in a student's record. This includes, but is not limited to:

- Grades
- GPA
- Transcripts
- Report Cards
- Family Contact Information
- Course Schedules
- Physical Testing Results
- Attendance Records
- Immunization and Medical Records
- Disciplinary Records
- Special Education Records
- Psychological evaluations

Student Righs Under FERPA

Both "eligible" students (18 and above), as well as their parents, hold the right to scrutinize, and request corrections changes to education records maintained by the school. They also have the right to forbid schools from disclosing information and obtain the school's procedure concerning educational records.

The policy informs them about how to:

- Request to review and correct records
- Refuse (or consent) to disclose directory information
- File a complaint about violations

Student Righs Under FERPA

While prior permission is required to disclose information, schools may reveal records without consent from either the eligible students or their parents in some situations.

The policy informs them about how to:

- Request to review and correct records
- Refuse (or consent) to disclose directory information
- File a complaint about violations

Who Doesn't Come Under FERPA

While prior permission is required to disclose information, schools may reveal records without consent from either the eligible students or their parents in some situations.

Schools can lawfully disclose information to:

- school officials with legitiamte reasons for accessing the information
- educational institutions where students plan to enroll
- federal authorities for purposes of evaluation or audit
- for awarding students financial aid
- local authorities within a juvenile justice system
- the parents of a dependent student
- health or safety services in connection with a health emergency

Partner With Compliant Vendors

Educational institutions must ensure that their third-party vendors are FERPA compliant. They are held accountable for all intentional (and unintentional) misuses of student information.

Train Your Staff and Faculty

Education institutions should conduct yearly FERPA training, including how staff should convey the rights it provides to students and their parents. School staff also need to know when and how to discuss student information and with whom.

Adequate training can significantly reduce many of the FERPA violations that occur daily and how to enable students and parents to access their education records.

Implement Compliance Policies and Best Practices

Implement new policies and procedures that comply with FERPA so that staff and administrators have a clear picture of what is legally permitted – and what isn't.

Consequently, a data breach response plan can outline how staff can minimize compliance risks by tightening access to sensitive information. Compliance policies should also include best practices, such as not sharing confidential information over email.

Well formulated policies can help to mitigate the damage caused by data breaches or unauthorized disclosure. When administrators are trained to handle student information carefully, it makes it easier for schools to comply.

Encrypt Emails and Sensitive Files

While compliance experts frequently advise schools to refrain from sharing sensitive information over email, it is one of the most common forms of staff communication within educational institutions. It allows for the unprotected transmission of sensitive information.

Encryption provides an extra layer of protection and gives staff the tools they need to keep student data secure, as files cannot be accessed without a decryption key.

Implement Prevention Tools and Software

While the administration is directly responsible for ensuring compliance, IT staff and teaching faculty will also need to make a consolidated effort in minimizing the vulnerability of student information.

So, if the administration stores student information on the cloud, routine scans will help to identify gaps and protect records from misuse. Should any be found, the IT team can mitigate issues and work with teachers to eliminate the risk of data breaches.

Here, the administration can install compliance-monitoring software on school hardware to monitor how the staff interacts with directory and PII, and instantly be alerted to suspicious behavior when handling sensitive files.

Read more about FERPA compliance here.

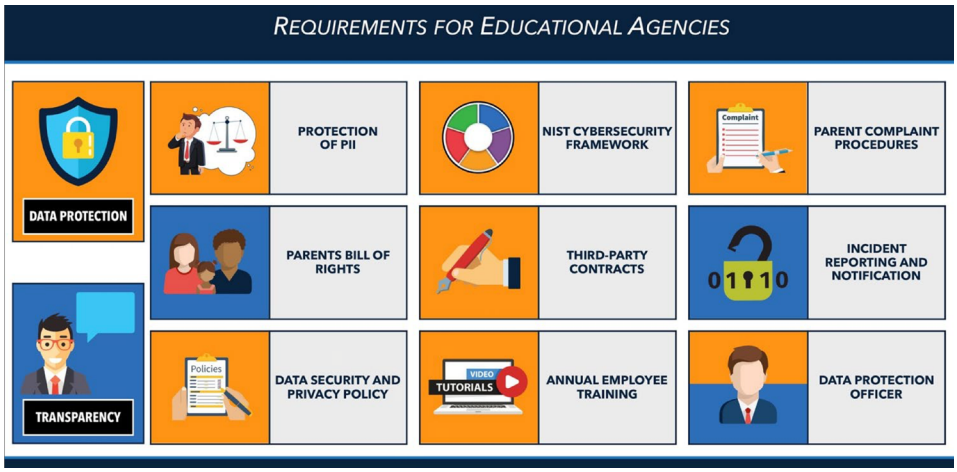
Education Law Section 2-D

Applicable to educational institutions, school districts, and boards of cooperative education in New York – the Education Law Section 2D aims to foster the security and privacy of any/all PII of students. Student information protected includes, but is not limited to:

- Name of the student or the names of their family members
- Residential address of the student or their family
- PII such as a student's social security number
- Indirect identifiers such as their mother's maiden name
- Information that allows school community members (with no prior knowledge of relevant circumstances) to identify a student with confidence
- Information requested by an individual that the educational institution believes to knows the identity of the student to whom the record relates

Education Law Section 2-D also protects the information privacy of teaching staff and administrative staff like the principal. Here, the Act secures confidential information such as annual performance review data of principals and teachers as well as their PII.

Read more about compliance with the Education Law Section here .



Source: Regional Information Center

Implement Prevention Tools and Software

COPPA was initiated as a measure to combat aggressive marketing techniques that target children – at a time when websites were collecting data on children without parental consent.

With COPPA now in place, website owners and operators need to abide by guidelines that dictate how this information is collected and maintained. These mandate:

- Websites are required to obtain parental consent before they collect personal information from minors (under-13 website users).
- How website operators should frame their privacy policy, including where this policy is posted on the website.
- When and how verifiable parental consent is to be sought.
- Restrictions on vigorous marketing techniques that operators use in regards to the information they collect.

Determine the Collection of Personal Information from Children Under 13

Given that COPPA's main aim is to protect children from aggressive online advertising, not all websites are subject to compliance.

The Federal Trade Commission (FTC) considers a wide range of factors before it classifies a website or online service under the jurisdiction of the Act. This includes content that is directed to children under 13, including subject matter, visual and audio content, and the use of child-oriented animations and incentives.

That said, any/all websites that collect the personal information of children under 12 are required to comply with COPPA. Compliance with COPPA is necessary if:

- An online service or website targets and manages the personal information of children under 13
- An online service or website targets children under 13 and permits third-party services to gather their personal information
- Your website targets a general consumer audience, but also collects personal information from children under 13

Websites and Online Services

Along with standard websites, online services that are required to comply with COPPA include:

- mobile apps that send or receive information online (apps that deliver targeted ads)
- network-enabled gaming platforms
- plug-ins
- advertising networks
- location-based services
- internet of Things (IoT) devices or connected toys
- purchase online goods or services
- smart speakers and voice assistants

Data Collection

Under COPPA, you collect personal information if you:

- prompt or encourage users (even through optional means) to submit their personal information
- allow consumers' data to be made public
- passively track a child's online activity

Verifiable Parental Consent

Before website operators collect, use, or disclose personal information from a child, they need to obtain their parent's verifiable consent. They have unlimited means to do this, but ultimately need to certify that the individual consenting to the data collection is, in fact, the child's parent.

Acceptable methods of obtaining verifiable parental consent include having a parent:

- sign a consent form that they can return via mail, fax, or electronic scan
- provide a scan or copy of their government-issued ID or driver's license that you verify against a database
- pay through online payment options such as a debit or credit card where they can track future transactions through notifications
- call a toll-free number answered by your staff
- connect to your staff via video call or chat

Read more about COPPA compliance here.

What Personal Information is Protected Under COPPA?

As defined in 16 C.F.R. § 312.2, personal information includes:

Endnote

The amount of student data that is collected and recorded on the daily continues to soar. Combined with the growing use of technology among children, it's become more difficult for schools to comply with privacy and information protection laws that guide them.

Schools that fail to meet compliance may be threatened with disciplinary action such as fines and lawsuits – or worse yet – they may be forced to forfeit federal funding.

With minute details that are easy to miss, educational institutions need to be able to respond to compliance issues and avoid facing risks. Building on the high standards of student data privacy is the only way schools can ensure and maintain their compliance.

Computer Resources of America: Your Compliance Solution

As one of the leading IT providers for the education industry, CRA specializes in delivering tailored solutions for schools and classrooms, both physical and virtual.

Led by our almost three decades' worth of experience, we strive to deliver exceptional workplace technology solutions that help educational entities streamline their overall processes – as well as cut down operating overheads and focus on their organizational goals and objectives.

As the go-to managed service provider (MSP) for a variety of technology solutions for calssrooms, we utilize our industry knowledge to carve out the best solutions so schools they focus on what they do best with ease of operations and peace of mind.

Interested in learning more? Contact us now.

CRA™ Transform IT
Computer Resources of America

Corporate Headquarters

64 West 48th Street, New York, NY 10036 – 212-376-4040 – www.consultcra.com – hello@consultcra.com