Enabling FERPA Compliance with Virtru

What is FERPA?

The Family Educational Rights and Privacy Act (FERPA) sets rules for how federally-funded educational institutions can disclose educational records. While the policy doesn't allow parents to sue institutions violating FERPA, the institution can lose federal funding if it does not comply with FERPA guidelines.

Who does FERPA affect?

All public and private educational organizations must comply with FERPA to protect student records, which may include such indicators as:

- **Dates of birth**
- **Addresses**
- **Social security numbers**
- **Grades and test scores**
- **Special education records**
- **Disciplinary records**
- **Medical and health records**
- **Attendance records**
- **Academic credit taken**
- **Degrees obtained**

What Are the Encryption Requirements? How Does Virtru Help?

Topic	FERPA Requirements	Relevant Virtru Features
Access Control	Student records can only be seen by authorized individuals	AES-256 bit encryption; Message revocation; Forwarding control; Message read receipts
Access Documentation	Upon request, institutions must disclose who has seen student records	Read receipts; E-discovery of encrypted content
Data Breach Disclosure	If an unauthorized individual gains access, the student or guardian must be notified.	Message read receipts

Going Beyond the Requirements

In addition to these requirements, Virtru provides other valuable security and control capabilities for organizations looking to comply with FERPA:

- **Persistent Access Control –** Revoke access to student records shared inadvertently, or set message expiration periods when communicating with recipients who do not require long-term access to sensitive information.
- **Message Audit –** See when messages are forwarded and revoke access at any point to ensure that only authorized recipients can access student records.
- **Data Loss Prevention (DLP) –** Customizable DLP rules allow organizations to automatically detect and encrypt student records before they leave the domain.
- **Customer-Hosted Encryption Keys –** Virtru's Customer Key Server (CKS) allows educational institutions to choose where their encryption keys are located. As a result, they can ensure that keys stay within the United States, while also preventing third party cloud providers from ever accessing their unencrypted data.
- **Search and E-Discovery –** Unlike S/MIME and PGP, Virtru's client-side encryption keeps messages searchable and exportable for Freedom of Information Act requests, audits, or other e-discovery requirements.

Have more questions about FERPA encryption requirements?

Contact sales@virtru.com today to speak with one of our compliance experts.

More Than 6,000 Organizations Have Made the Switch to Virtru