Security Compliance

eReserve is committed to keeping your data private and secure.

eReserve's privacy practices, technical controls, and security measures are designed to protect the data its customers submit to eReserve Plus, referred to as "Non-Personal Customer Data", as well as maintaining separation from student educational records

FERPA Compliance

What is FERPA?

FERPA is a United States federal law that protects the privacy of students in their educational records from unauthorized disclosure. Rights under FERPA transfer from the parents of a student to the student when the student turns 18 years of age or enrolls in school beyond the high school level at any age. FERPA applies to all academic institutions that receive funds from a Department of Education program.

What are educational records? FERPA classifies educational records as records that directly relate to a student and are maintained by an educational agency, academic institution, or by a party acting for the agency or institution.

Is there a FERPA certification? There are not currently any certification programs approved by the federal government that assess third-party compliance with FERPA. Academic institutions must perform their own assessments to determine whether a third-party product or service affects their compliance.

Here’s how eReserve supports customers with their FERPA compliance.

Cybersecurity Framework
eReserve Plus complies with the International Organization for Standardization 27001 (ISO 27001) security framework, applying the necessary information security compliance standards.

ISO 27001 certification issued by QMS Certification Services, No. 500-05911-IS, valid to 22/11/2025.

Data Security
eReserve Plus supports the latest recommended secure, up to date, strong cipher suites and protocols to encrypt Customer Data in transit and at rest, including HTTPS and SSH. eReserve also perform regular vulnerability scans and application-level penetration tests by independent entities.

Data retention and disposal
Non-Personal Customer Data is removed from production servers nightly following deletion by the end user, and is then permanently deleted from backup within 14 days in line with best practices.

Customer Data Privacy
The content of student educational records connected to eReserve Plus is not monitored and all data can be purged on request.

Data export is provided only on request, and destruction beyond normal expiration of already encrypted content is only via request.

Transparent security and privacy practices
eReserve Plus' policies and practices are customer-conscious, and transparent. Our security practices and privacy policy are publicly available. Customers can review our

third-party audit reports upon their request (and they are available to potential customers after signing an NDA).

Subprocessor Transparency
eReserve Plus data is only directly accessed by institutions via the secure eReserve API. Third parties are provided data via institution controls.

eReserve is also transparent about our third-party data processors that help support the delivery of eReserve Plus with whom we share Non-Personal Customer Data. A list of our current third-party data processors includes:

- BlackBoard
- Moodle
- Semaphore
- Papertrail
- Sentry
- SendGrid

Physical Safeguards
Industry standard cloud infrastructure provided and heavily documented by AWS provides data segregation for individual institutions and environments with layered hierarchical access controls. All machine images are audited and running programs logged.

Amazon Web Services (AWS) is our third-party hosting provider. AWS has world-class physical and environmental security, including strictly controlled perimeters, ingress points with video surveillance, on-site security, and two-factor authentication. More on AWS's physical and environmental security is available here.