FERPA-Aligned Student Data Protection Addendum (SDPA)

Last Updated: November 2025

This FERPA-Aligned Student Data Protection Addendum ("Addendum") applies when an educational agency or institution ("Institution") uses GradeBot to process Student Data subject to the Family Educational Rights and Privacy Act ("FERPA"). This Addendum supplements the GradeBot Terms of Service and governs GradeBot's processing of Student Data on behalf of the Institution.

1. Definitions

- **"GradeBot"** means the GradeBot platform and the service provider operating it.
- **"Institution"** means the educational agency or institution using GradeBot.
- **"Student Data"** means any information contained in documents or records uploaded to GradeBot that is directly related to an identified or identifiable student or applicant and maintained on behalf of the Institution.
- **"School Official"** has the meaning given in FERPA and includes a contractor or service provider performing institutional services or functions with a legitimate educational interest.
- **"De-Identified Data"** means data that cannot reasonably be used to identify a student.
- **"Grading Session"** means the period during which an instructor uploads documents, configures grading or review options, and runs automated evaluation or feedback processes for a given cohort, assignment, or applicant set. A grading session ends when the instructor explicitly exits the session in the interface or when 24 hours have passed since the session was created, whichever occurs first.

2. FERPA Status and Role

When used by a U.S. educational Institution, GradeBot is designated as a **School Official** under FERPA and:

- Performs institutional services (grading, evaluation, and screening) for which the Institution would otherwise use its own employees
- Has a legitimate educational interest in Student Data solely to perform those services

- Is subject to the Institution's direct control with respect to the use and maintenance of Student Data, as described in this Addendum and any written institutional agreements

3. Purpose and Use Limitations

GradeBot will use Student Data only to:

- Evaluate and score assignments, essays, or application materials
- Generate feedback, summaries, and screening recommendations
- Perform OCR, text extraction, and related document processing
- Provide security, logging, and operational support related to the grading session
- Comply with legal or regulatory obligations, when applicable

GradeBot will **not**:

- Sell Student Data
- Use Student Data for targeted advertising
- Use Student Data to train generalized models or foundation models
- Use Student Data for analytics unrelated to system operation, security, or performance

Student Data remains at all times the property of, and under the control of, the Institution.

4. Data Retention and Deletion

4.1 Short-Term Storage of Student Data

GradeBot stores Student Data only for a limited time and only as necessary to complete grading sessions.

- Uploaded student or applicant documents are stored in encrypted Azure Blob Storage under session-specific paths.
- Extracted text, OCR results, and intermediate processing artifacts are stored in short-lived storage associated with grading sessions.

Retention limits:

- Uploaded documents are automatically deleted within **24 hours** of grading session creation or sooner when the instructor explicitly exits the grading session.
- Extracted text, OCR results, and intermediate processing data are automatically deleted within **24 hours** or when the grading session ends, whichever occurs first.

Student documents and extracted Student Data are not stored in long-term backups or analytics systems.

4.2 Long-Term Records

GradeBot may retain long-term records that do not include student documents or full extracted

Student Data, such as:

- Instructor accounts and role assignments
- Assignment, rubric, and cohort configurations
- Usage metrics and de-identified operational metadata
- Security and audit logs that record actions (for example, login events, exports, configuration changes)

These long-term records are designed not to contain Student Data, except possibly in de-identified or pseudonymous form.

4.3 Deletion at Institution's Direction

Because Student Data is automatically deleted on a short-term schedule, no additional deletion is usually required. If the Institution believes Student Data remains in GradeBot beyond the described retention periods, GradeBot will reasonably cooperate to investigate and, if necessary, delete or de-identify any remaining Student Data under the Institution's direction.

5. Security and Safeguards

GradeBot will maintain administrative, physical, and technical safeguards designed to:

- Protect Student Data from unauthorized access, disclosure, alteration, or destruction
- Ensure the confidentiality, integrity, and availability of processing systems

These safeguards include:

- TLS/HTTPS encryption for all network communications
- Encrypted storage on Azure services, including Blob Storage and PostgreSQL
- Role-based access control and authentication via Microsoft Entra / Microsoft Entra ID
- Scoped SAS tokens for Blob access
- Structured audit logging for security-relevant and administrative events
- Containerized infrastructure and environment-based configuration management

GradeBot's personnel will access Student Data only when necessary to perform support, maintenance, or security functions on behalf of the Institution and are bound by confidentiality obligations.

6. Subprocessors and Third-Party Providers

The Institution authorizes GradeBot to use the following subprocessors in connection with

Student Data, solely for the purposes described in this Addendum:

- **AI Providers:** OpenAI Enterprise and Google Gemini Enterprise, for text analysis, scoring, and feedback generation
- **OCR Provider:** Azure Document Intelligence, for PDF and image text extraction
- **Authentication Provider:** Microsoft Entra ID, for identity and access management
- **Cloud Infrastructure:** Microsoft Azure, for hosting, storage, and network services

These subprocessors operate under enterprise agreements that impose confidentiality obligations and prohibit using Institution-controlled Student Data to train generalized AI models or for unrelated purposes. GradeBot will maintain a list of subprocessors and, where required by law or contract, notify the Institution of material changes.

7. Access and Control

The Institution retains full control over Student Data and:

- Determines which Users are authorized to upload and process Student Data
- Configures roles and permissions (for example, instructor, admin, read-only)
- Controls the initiation and scope of grading sessions
- Controls exports of grading results that may contain Student Data

Students must submit requests to access, correct, or delete their educational records through the Institution. GradeBot will reasonably cooperate with the Institution in fulfilling such requests consistent with the short-term retention model and technical capabilities of the service.

8. Data Location and International Transfer

Student Data is processed and stored in Microsoft Azure regions selected at deployment time by or for the Institution. GradeBot will not intentionally move Student Data outside the chosen regions except:

- As required by the Institution
- As necessary for disaster recovery in equivalent or nearby regions, subject to applicable agreements
- As required by law

Where data transfers are subject to additional legal requirements (for example, GDPR), GradeBot and the Institution will cooperate in implementing appropriate safeguards.

9. Breach Notification

If GradeBot confirms unauthorized access to or disclosure of Student Data in its possession or control ("Security Incident"), GradeBot will:

- Notify the Institution without unreasonable delay after becoming aware of the Security Incident
- Provide available information about the nature of the incident, the affected data (to the extent known), and steps taken or planned to mitigate the impact
- Cooperate with the Institution's reasonable requests for information needed to meet its own legal and regulatory obligations

The Institution is responsible for determining whether to notify affected individuals, regulators, or other third parties, unless otherwise required by law.

10. Termination of Services

Upon termination or expiration of the Institution's access to GradeBot:

- Institution User access to the platform will be disabled
- Student Data will already have been deleted according to the short-term retention schedule described in Section 4
- Instructor and system records that do not contain Student Data may continue to be retained as described in this Addendum and the Privacy Policy

If the Institution believes Student Data remains in GradeBot after termination, it may request confirmation and, if necessary, deletion of any residual Student Data consistent with technical feasibility and applicable law.

11. Conflict of Terms

In the event of a conflict between this Addendum and the GradeBot Terms of Service regarding the handling of Student Data, this Addendum will control to the extent of the conflict. In all other respects, the Terms of Service remain in full force and effect.

12. Contact

For questions about this Addendum, FERPA compliance, or Student Data protection in

GradeBot, the Institution may contact:

admin@gradebot.ai