FERPA Compliance on First Draft's Learn Platform

Last Edited January 3rd, 2023

Executive Summary

As an Education Technology company, First Draft LLC places the utmost importance on data privacy and protection. This document outlines our commitment to safeguarding Personally Identifiable Information (PII) and our compliance with the Family Educational Rights and Privacy Act (FERPA) in our learn.First Draft.com ("Learn") platform. We detail our approach to data security, governance, and encryption to ensure the confidentiality, integrity, and availability of student information.

Our FERPA statement, Terms of Service, and Privacy Policy on First Draft's Learn platform complement the summary of our data privacy and FERPA compliance outlined in this document.

FERPA Compliance

FERPA is a federal law designed to protect the privacy of student education records. At First Draft, we understand and adhere to the key FERPA requirements:

1. **Protection of Student Records**: Student educational records with Personally Identifiable Information (PII), including various identifiers directly or indirectly tied to an individual, are handled with care internally and never disclosed externally with some exceptions.

2. **Authorized Disclosures:** Student records can be disclosed without express written consent of the student, or their guardian if the student is less than 18 years old, in these cases:

    - School officials with legitimate educational interest;
    - Other schools to which a student is transferring;
    - Specified officials for audit or evaluation purposes;
    - Appropriate parties in connection with financial aid to a student;
    - Organizations conducting certain studies for or on behalf of the school;
    - Accrediting organizations;
    - To comply with a judicial order or lawfully issued subpoena;
    - Appropriate officials in cases of health and safety emergencies;
    - State and local authorities, within a juvenile justice system, pursuant to specific state law.

3. **Parent and Student Rights:** Parents and eligible students have the right to inspect and review education records, request amendments, consent to disclosures, and file complaints.

Security Guidelines at First Draft

First Draft prioritizes data security using the US Department of Education's Privacy Technical Assistance Center (PTAC) Data Security Checklist to:

- Develop a comprehensive data governance plan with clear policies for PII protection, including established procedures for containing and fixing security incidents.
- Integrate security into every level of our application, and conduct regular compliance checks.
- Utilize physically secure computing resources.
- Employ a layered defense architecture with encryption of data in transit, at rest, and at the application level.
- Use a robust web application framework for developing and deploying our services, including regular security software updates to address vulnerabilities.
- Enforce strong passwords, and role-based access.
- Establish clear roles and responsibilities for data access.

Furthermore, First Draft follows the PTAC Data Governance Checklist to:

- Document operational needs justifying data collection, regularly reviewing and revising data content management policies.
- Implement mechanisms for de-identifying PII and establish policies for handling records throughout the data lifecycle.
- Implement policies and procedures for restricted and monitored data access, including procedural controls and training.
- Develop a comprehensive security framework, conduct risk assessments, monitor and audit data security regularly, and establish policies for data exchanges and reporting.

Encryption and Data Access on the Learn Platform

Encryption at Rest and Database Backups

Encryption at rest safeguards against unauthorized access to the file system. First Draft ensures the security of data through daily Advanced Encryption Standard 256-bit (AES-256), block-level encrypted backups, stored and managed in a secure Amazon Web Services S3 bucket in the US region via our application hosting provider, Heroku. This protects against unauthorized access to backup files. The FERPA compliance of Amazon Web Services is available online.

Encryption in Transit

First Draft uses TLS/SSL to encrypt data in transit, providing end-to-end encryption and integrity for all web requests. SSL and TLS protocols protect against potential eavesdropping over the network. Automated certificate management is utilized to automate SSL security processes.

Encryption at the Application Level

First Draft goes beyond industry standards of encryption at rest and in transit by encrypting sensitive database information at the application level with AES-256 encryption. This additional layer of encryption protects against:

- Reading or tampering with sensitive fields if the database is inappropriately accessed.
- Accidentally exposing sensitive data in logs.

The sensitive data encrypted at the application level includes any user PII.

FERPA Training and Student Data Access at First Draft

At First Draft, we collect the following PII from students, primarily for connecting educational records (i.e. lessons and grades) with identities:

- Email address
- First and last name

First Draft employees with access to sensitive student PII are FERPA trained. Any employees without FERPA training undergo audits conducted by FERPA-trained staff when accessing sensitive student data, e.g.: during maintenance activities involving queries or displays of PII, which are recorded and audited.

Third-Party Services

First Draft ensures the anonymization of user PII when using third-party services, such as application analytics.

Conclusion

First Draft is dedicated to protecting student data privacy, upholding FERPA compliance, and employing advanced encryption practices for all user data in our learn.First Draft.com (“Learn”) platform. By adhering to the highest standards, we provide a secure and compliant environment for the educational community.