DATA PRIVACY CONSIDERATIONS FOR AN AI-POWERED EDUCATIONAL ASSESSMENT APPLICATION - CRITIQUIZ

In developing an AI assessment tool such as CritiQuiz and having it focus on middle school students, prioritizing data privacy to follow legal standards to protect minors and personal information in general is very important. Some of the laws we will be taking into consideration in particular are the Children's Internet Protection Act (CIPA), the Children's Online Privacy Protection Act (COPPA), and the Family Educational Rights and Privacy Act (FERPA) to protect students' private information and online experiences. Here we will address the standard procedures that apply to our app CritiQuiz, the possible dangers of data compliance, and the safeguards we want to put in place to guarantee the greatest level of security and privacy for our users.

The Family Educational Rights and Privacy Act is a federal law that protects the privacy of student educational records (20 U.S.C. § 1232g; 34 CFR Part 99). FERPA gives parents specific rights concerning their children's education records until the student reaches 18, when those rights transfer to the student. In the context of our app, this means we must carefully control any information that could personally identify students such as names, performance data, and quiz responses ensuring that data is accessible only to authorized personnel with a legitimate educational interest (U.S. Department of Education, 2023). FERPA also requires that guardians give explicit permission before schools or applications share / use student information for purposes beyond education, which simply highlights the need for secure access and limited data visibility within our application.

Another relevant law to our app CritiQuiz is the Children's Online Privacy Protection Act (COPPA) which governs the collection of personal information from children under 13. Since our application will cater to middle school students, we anticipate some users may be under this age threshold. COPPA mandates that online services targeting children obtain verified parental consent before collecting any personally identifiable information (15 U.S.C. § 6501; Federal Trade Commission, 2023). This kind of requirement is crucial in establishing trust with guardians and ensuring that they understand what data is collected and how it will be used. Once the app is in use, we will have to present parents with a clear and accessible consent form that outlines our data collection practices, the educational purpose behind our AI-powered feedback, and options for parents to access, review, or request the deletion of their child's data at any time.

Another consideration is the Children's Internet Protection Act (CIPA) which further enforces protective measures for minors by requiring educational institutions to safeguard students from harmful online content (47 U.S.C. § 254; Federal Communications Commission, 2023). Although this regulation applies mostly to schools receiving federal funding for their internet

access, our application's alignment with CIPA principles will be essential in creating a safe digital learning environment for young internet users. Our AI's content will be carefully designed to provide only age-appropriate feedback, and we will implement strict filters to prevent any unintended exposure to harmful material. By adhering to CIPA guidelines, education success remains the focus of CritiQuiz.

Given the sensitive nature of student data, several risks must be thought of and assessed. Unauthorized access to educational records poses a significant threat to our app if the correct security measures are not in place. If the collected data were to be viewed by someone that it was not minted for, it could lead to identity theft, targeted advertising, or misuse of educational records. Similarly, as an AI-driven platform, our application requires student data to function adaptively. This brings up the challenge of ensuring data is not unnecessarily stored or processed beyond educational purpose, as doing so could violate FERPA's and COPPA's data retention and limited-use mandates (U.S. Department of Education, 2023; Federal Trade Commission, 2023).

Another critical risk is the unintended collection of sensitive information. AI-driven feedback can occasionally prompt students to share personal details in their responses, capturing data that falls outside the educational sphere. This risk is essential to be aware of in an environment where responses are designed to promote critical thinking, which might lead students to express personal reflections that exceed the boundaries of typical quiz data. To address these risks, we are implementing a series of robust measures to comply with data privacy regulations and protect student information.

Limited Data Collection and Use: Our data collection approach is very minimalistic, aligning with the principle of data minimization outlined in FERPA and COPPA. We collect only the data necessary for educational assessment, such as student performance on quizzes or exams, progress tracking, and general feedback on responses. Personal identifiers like student names will be stored separately from assessment data, accessible only to school officials with legitimate educational interests and proof of such (U.S. Department of Education, 2023). Performance data, while essential for the app's adaptive feedback feature, will be anonymized where possible to further protect student identity and ensure that no extraneous PII is collected or retained.

Parental Consent Process: We have created a permission form that is transparent and easy to understand in order to comply with COPPA's requirement for verified parental consent. This document will outline the kinds of information gathered, the objectives of each data category, and the steps taken to safeguard the privacy of students (Federal Trade Commission, 2023). Details on how parents can exercise their right to see or remove their child's information will also be included as well. In order to streamline the consent process, our application will offer a user-friendly onboarding experience that walks parents through these conditions, empowering them to make knowledgeable decisions and access their child's data whenever they choose.

Data Access Controls: All student data will be protected using industry-standard encryption algorithms both in transit and at rest to reduce the possibility of unwanted access. Security is the cornerstone of safeguarding student privacy. This makes sure that even in the event that data is intercepted, it will be safe and unreadable by unauthorized users. Access to student data will also be role-based, meaning that only administrators, technical staff, and authorized teachers with particular rights would be able to see or manage student records. By putting these role-based access restrictions in place, we guarantee FERPA's restricted access criteria are met and drastically lower the danger of data disclosure. (U.S. Department of Education, 2023).

Data Anonymization and Retention Policies: To prevent the unnecessary accumulation of student data, we will anonymize data used for AI-driven analytics and restrict data retention periods. By removing personally identifiable details from performance analytics, we protect student identities while still enabling the AI to improve its adaptive feedback mechanisms. Moreover, our platform will implement an automatic data deletion policy to remove stored information after a specific period unless extended retention is necessary for educational data purposes. This retention policy will be transparent to users, reinforcing our commitment to limited data usage in compliance with FERPA and COPPA guidelines (Federal Trade Commission, 2023).

Transparency and Age-Appropriate Content: Our AI's comments and input will be rigorously adapted to middle school academic standards in accordance with CIPA's recommendations about content suitability. We are always reviewing AI prompts to make sure the information is age-appropriate and constructive—all of which are consistent with our dedication to responsible and safe educational technology. To increase openness, our privacy policy will be made publicly available, including our data collection procedures, content standards, and user rights in language that parents, teachers, and students can all understand. (Federal Communications Commission, 2023).

We are committed to creating a secure, student-development-promoting AI-powered assessment platform by adopting a proactive, regulatory-compliant approach to data protection. We are dedicated to keeping middle school pupils in a secure and beneficial learning environment by implementing age-appropriate content guidelines, robust encryption, verifiable parental consent, and careful data gathering and minimization. This commitment not only fulfills legal requirements but also supports the ethical development of our platform, ensuring we uphold the trust placed in us by students, parents, and educators.

References

Federal Communications Commission. (2023). *Children's Internet Protection Act (CIPA) Compliance Guidelines*. Retrieved from https://www.fcc.gov

Federal Trade Commission. (2023). *Children's Online Privacy Protection Act (COPPA) FAQs*. Retrieved from https://www.ftc.gov

U.S. Department of Education. (2023). *FERPA Regulations: Family Educational Rights and Privacy Act (FERPA) Compliance and Guidelines*. Retrieved from https://www.ed.gov