Student Data Confidentiality and Privacy Policy

Social Studies School Service

Table of Contents

Effective Date: April 1, 2025

1. Introduction

This Student Data and Privacy Policy outlines how we collect, use, and protect data in compliance with FERPA, COPPA, and any applicable state data privacy regulations. We are committed to protecting the safety and privacy of our users, including students, educators, and school districts and demonstrate this by using the principles of data minimization, purpose limitation, and transparency. This policy covers all the data processed through our Learning Management System (LMS) and associated AI functionalities.

2. Definitions

2.1 Data: Refers to all Personally Identifiable Information (PII) and non-public information collected through our platform, including (but not limited to) student names, user IDs, assessment results, discussion posts, and any metadata generated by our LMS or AI tools.

2.2 Ownership: The school or district retains ownership of student data. We do not claim ownership of student data.

2.3 Data De-Identification: We may use fully de-identified data—having removed all personal identifiers—for research or product development purposes. We will not attempt, nor allow third parties to attempt, to re-identify this data. Any such usage is limited to improving our services and will never be shared in a manner that permits re-identification.

3. Data Collection and Usage

We collect various types of data to enhance your educational experience and ensure our services are effective. Below is an overview of the types of data we collect, how it is used, and how we handle it.

3.1 Types of Data Collected

- **Personal Information**: Includes student names, teacher identifiers, grade levels, and any other personally identifiable information (PII).

- **Academic Data**: Includes student progress, responses to assessments, grades, and other academic records generated within our LMS.

- **AI-Specific Data**: Student first names and inputs provided during AI-driven interactions (chatbot prompts, feedback texts) used to improve and personalize learning.

3.2 How We Use Data

- **Educational Enhancement**: We use data to personalize learning experiences, adjust assignments based on a student's grade and readiness, and offer feedback to help students improve.

- **AI Functionality**: Our AI tools, including Large Language Models (LLMs), use data to improve chatbot interactions, automate grading, and offer more tailored learning support. Data is anonymized when used to train models.

- **3.3 Data Sharing**

  - **Third-Party Sharing**: We do not share any data collected with third parties for commercial purposes.

  - **Data Hosting**: All data is securely stored on servers located within the United States.

3.4 Compliance with Laws

We comply with all relevant state and federal laws, including the **Family Educational Rights and Privacy Act (FERPA)** and the **Children's Online Privacy Protection Act (COPPA)**, as well as applicable state-level student data privacy regulations, to ensure that student data is protected.

3.5 Confidentiality and Data Limitation

  - **Confidentiality**: We take steps to maintain the confidentiality of student data and ensure it is only accessible to authorized personnel.

  - **Data Minimization**: We collect only the data necessary to provide our educational services, and we do not use student data for any other purpose.

4. User Consent and Control

We are committed to transparency and user control over data.

4.1 Obtaining Consent

We work directly with school districts to establish agreements that outline how student data is collected and used. These agreements ensure compliance with all federal and state privacy laws and transparency.

4.2 User Control

  - **Opt-Out Options**: Currently, users cannot opt out of data collection, as the data is essential for the functioning of our educational services. The data collected is solely related to student performance and is not used for any other purposes.

  - **Data Usage Limitation**: All data is used exclusively for educational purposes and is not shared with third parties.

  - **Data Removal**: School districts can request the removal of specific student data by contacting us at help@socialstudies.com. Parents or guardians should route requests through their district.

5. Security Measures

We take the security of student data seriously and implement robust measures to protect it.

5.1 Data Protection Protocols

  - **Encryption**: All data is transmitted securely using SSL encryption to protect it in transit. Sensitive information, such as passwords, is also encrypted when stored.

- **Server Security**: Our servers are in physically secure data centers in the United States with advanced firewalls and intrusion detection systems to prevent unauthorized access. We continuously monitor threats and apply regular security patches.

- **Access Controls**: We use role-based access to ensure only authorized personnel can view sensitive information. Additionally, all employees with access to student data undergo privacy and security training.

5.2 System Integrity

We follow best practices for securing systems, including using strong passwords and email verification processes.

5.3 Incident Response

In the event of a data breach, we will notify affected school districts within 24 hours, providing details about the compromised data and the steps taken to mitigate the breach.

5.4 Security Audits

We regularly perform security audits to identify and address potential vulnerabilities.

6. AI Functionality and Decision-Making

Our platform uses AI to improve learning experiences. Here's how AI is used and how we ensure fairness.

6.1 Personalized Learning

Our AI system helps personalize lessons by recommending resources like videos, charts, and assignments based on student performance and readiness.

6.2 Automated Grading

AI helps grade student responses by comparing them to correct answers and providing feedback to help students improve.

6.3 Transparency

While AI supports grading and learning recommendations, most grading criteria and suggested answers are defined by human educators to ensure fairness and clarity.

6.4 AI Fairness and Bias Mitigation

We regularly audit our AI algorithms to ensure fairness and minimize bias based on race, gender, ethnicity, or other protected characteristics.

6.5 Use of Student Data for AI Training

We may use anonymized, aggregated student data to improve our AI technologies, including Large Language Models (LLMs). This data is not personally identifiable and is only used to improve our educational systems.

7. Compliance and Governance

We adhere to all applicable regulations and ensure that our practices meet the needs of each school district.

7.1 Regulatory Compliance

We fully comply with laws such as FERPA, COPPA, and HIPAA to protect student data.

7.2 Adherence to Policies

We follow agreements with school districts to ensure that data collection and usage meet specific district requirements.

7.3 Prohibited Practices

- **Data Selling**: We do not sell student data.
- **Advertising**: We do not use student data for advertising or targeted marketing.

7.4 Data Retention and Deletion

All student data is deleted at the end of the school year. No student data is carried over to the next year.

7.5 Addressing User Concerns

If you have concerns about data privacy, please contact our support team, and we will address them promptly.

8. Integration with Third-Party Services

We may offer integration with third-party services like **Google Classroom, Canvas, Schoology** and others. If you choose to integrate, you will need to grant access to certain student data (including student emails, assignments/coursework and student grades). This integration is secured and complies with all relevant privacy standards.

9. Privacy and Security Pledge

We uphold the following commitments:

9.1 Student Privacy Pledge

We have signed the Student Privacy Pledge, demonstrating our commitment to safeguarding student data and protecting the privacy and rights of students. By signing the pledge, we have agreed to:

- Not sell student data.
- Not use student data for targeted advertising.
- Use student data solely for educational purposes.
- Implement strong data security measures to protect student information.
- Be transparent about our data practices, allowing parents and guardians to review and request deletion of student data upon request.

9.2 Commitment to Cybersecurity Framework

We are fully committed to the privacy, confidentiality, and security of student data by adhering to established cybersecurity frameworks such as the **NIST Cybersecurity Framework (CSF) and CIS Controls.** We regularly review and enhance our cybersecurity practices to stay aligned with emerging threats and best practices, ensuring the highest level of protection for the data we manage.

10. Changes to This Policy

We may update this policy from time to time. If we make any significant changes, we will notify users and update the policy on our platform.

11. Contact Us

If you have any questions about this policy, please reach out to us:

- **Email**: help@socialstudies.com

- **Phone**: (800) 421-4246

- **Address**: PO Box 802, Culver City, CA 90232

- **Contact Person**: Dr. Aaron Willis, Chief Learning Officer

  awillis@socialstudies.com