METHODIST UNIVERSITY

Information Technology Policies and Standards

100.11	University Policy on Artificial Intelligence and Student Data	1 of 2
NUMBER	**TITLE**	**PAGE**

I. Policy Statement

This university **strictly prohibits the submission of protected student data to any artificial intelligence (AI) engine.** This includes, but is not limited to, any non-Methodist University authorized software or any online service that uses artificial intelligence for data analysis, processing, decision-making, or any tool that transforms data from voice recordings to text.

II. Rationale

This policy is rooted in the university's commitment to protecting the privacy and security of student data. This commitment is legally mandated by:

- **The Family Educational Rights and Privacy Act (FERPA):** FERPA is a federal law that protects the privacy of student education records. It grants parents and eligible students (those 18 or older or attending postsecondary institutions) various rights, including the right to inspect and review their education records, seek amendment of those records, and consent to the disclosure of personally identifiable information contained in those records.
- **The Gramm-Leach-Bliley Act (GLBA):** The GLBA is a federal law that applies to financial institutions, including higher education institutions that handle student financial records [6]. GLBA includes provisions that protect the privacy and security of consumer financial information, including student financial records such as tuition payments and financial aid records [6].

III. Scope

- **Protected Student Data:** This policy covers all information classified as "education records" under FERPA and "student financial records" under GLBA. This includes, but is not limited to:
    - Names, addresses, and contact information
    - Academic transcripts, grades, and test scores
    - Disciplinary records
    - Financial aid information
    - Disability status

- Any other personally identifiable information

- **AI Engines:** This policy applies to all non-MU-authorized AI-powered platforms, tools, and services, whether commercial, proprietary, or covered under an open-source license.

IV. Enforcement

Any violation of this policy will be subject to disciplinary action, up to and including termination of employment or expulsion from the university.

V. Compliance

- **FERPA:** Submitting protected student data to AI engines without proper consent could constitute an unauthorized disclosure of information, violating FERPA. FERPA does allow for disclosure of personally identifiable information without consent under specific circumstances, none of which cover the general use of AI engines.
- Exceptions to FERPA's consent requirement are narrowly defined and typically involve situations such as disclosures to school officials with legitimate educational interests, disclosures for financial aid purposes, or disclosures required by law. AI engines generally don't fall under these exceptions.
- Even in situations where disclosure might be permissible under a FERPA exception, universities must exercise caution to ensure that the AI engine provider has adequate security measures in place to protect the data and that the disclosure is limited to the minimum information necessary for the specific purpose.
- **GLBA:** Submitting student financial data to AI engines without appropriate safeguards would violate the GLBA's Safeguards Rule, which mandates institutions to implement security measures to protect consumer financial information.
- Universities must ensure that any AI engine used to process student financial data adheres to stringent security standards to prevent unauthorized access, use, or disclosure of this sensitive information.

VI. Additional Considerations

- **Data Security:** AI engines can be vulnerable to data breaches and cyberattacks. Universities must carefully assess the security practices of any AI engine before considering the submission of protected student data.
- **Transparency and Accountability:** It is crucial to ensure transparency in how AI engines use student data. Universities should require clear explanations of the data processing methods employed by these engines and hold providers accountable for responsible data handling practices.

- **Bias and Fairness:** AI algorithms can perpetuate and amplify existing biases. Universities must be vigilant in evaluating AI engines for potential bias that could unfairly disadvantage students.

VII. Conclusion

This policy is essential for protecting student privacy, maintaining compliance with federal regulations, and ensuring the responsible use of AI technology in the university setting. It is the responsibility of all university faculty, staff, and students to be aware of and adhere to this policy.