Resolution – Regulate EdTech

State of Texas Republican Party should adopt a platform plank to Regulate EdTech as follows:

> **Plank #xxx. Regulate EdTech:** In order to provide services to Texas schools, EdTech must be required to achieve certification for security assessment, privacy protection, and risk management similar to FedRAMP, StateRAMP, and TX-RAMP authorization. Schools shall not consent to data collection of minors on behalf of parents. Schools shall protect the confidentiality of students' identifiable information from unauthorized disclosure, commercial exploitation, and security breaches. Texas Legislature must codify federal privacy law with strong enforcement mechanisms without loopholes. We demand that the Texas legislature protect student data privacy by prohibiting the collection, distribution, and selling of data and the enforcement of data privacy through private right of action.

A copy of this resolution should be sent to the _____ County/Senate District #_____ Convention Resolutions Committee from Precinct #____ with the recommendation that it be passed and sent to the State Convention Platform Committee of the _____ Party of Texas.

Background

The Educational Technology market (**EdTech)** is **unregulated** and lacks a framework of management that protects children and prevents security breaches. Vendors routinely **contact educators and employees directly** to provide services and access **without oversight or management**. EdTech Law Center (https://edtech.law/) works to "protect students, parents, teachers, and schools from the **exploitative practices** of the EdTech industry" and have identified the following categories of abuse:

- Invasions of Privacy
- Harms to Health and Wellness
- Access to Inappropriate Content
- Unhealthy Agreement
- Data Insecurity
- Commercial Manipulation
- Discrimination
- No Access to Information
- No Consent

EdTech companies provide a broad range of services and products for the **school office, support structure, and classroom**. EdTech.Law Center (https://edtech.law/what-is-edtech/) has identified the following primary EdTech software and platforms:

- Behavior Monitoring/Surveillance Software (BMS)
- Classroom Messaging Software (CMS)
- College and Career Readiness Platform (CCR)
- Community Engagement Platform (CEP)
- Digital Learning Platform (DLP)
- Learning Management System (LeMS)
- Library Management Software (LiMS)
- Safety Platform (SP)
- School Management Software (SMS)
- School Transportation Software (STS)
- Single Sign On (SSO)
- Student Information System (SIS)
- Study Tools (ST)
- Virtual Classroom Software (VCS)

Technology companies comply with strong data privacy law in other countries and states such as: **European Union** (EU) General Data Protection Regulation (GDPR), **California** Privacy Rights Act (CPRA) of 2020, **California** Consumer Privacy Act of 2018 (CCPA), **Illinois** Student Online Personal Protection Act of 2019, and **New York's** Bill of Rights for Data Privacy and Security of 2015.

Technology companies comply with Federal and State Authorization programs in order to do business with federal, state, and local entities:

- Federal Risk and Authorization Management Program (**FedRAMP**) processes are required by federal law for cloud computing products and services used by federal agencies to provide a standardized approach to security assessment, authorization, and continuous monitoring. https://www.fedramp.gov/docs/authority/m-24-15/
- **StateRAMP**, also known as GovRAMP, is a voluntary, non-profit framework modeled after FedRAMP for state and local entities to standardize cloud security assessments and strict cybersecurity requirements. https://govramp.org/
- Texas Risk and Authorization Management Program (**TX-RAMP**), authorized by Texas Government Code § 2054.0593, provides a "standardized approach for security assessment, certification, and continuous monitoring of cloud computing services that process the data of Texas state agencies." https://dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp

Current **Federal** statutes provide **false security**, exist with **very little enforcement** to protect the confidentiality of a student's identifiable information, **allows schools to provide consent on behalf of the parents**, and enables schools to bully parents into a "**no-win, all or none**" choice on protection of privacy.

- 15 U.S.C. §§ 6501-6502 (16 CFR Part 312) Children's Online Privacy Protection Act (**COPPA**), enforced by the Federal Trade Commission (FTC), requires parental consent for minors to have access to **websites, online services, or apps** before **collecting, using, or disclosing personal information**. COPPA protection is limited to minors under age 13.
- 20 U.S.C. § 1232g (34 CFR Part 99) Family Educational Rights and Privacy Act **(FERPA)** requires parental consent before sharing **personally identifiable information** (PII) with **third parties**. FERPA's most significant loophole allows schools to establish vendors as a "legitimate educational purpose" and the vendors are not bound to FERPA requirements to protect data. Complaints regarding a violation in which a vendor has not been declared a "legitimate educational purpose" could be sent to the U.S. Department of Education.

- 20 U.S.C. § 1232h (34 CFR Part 98) Protection of Pupil Rights Amendment (**PPRA**), supposedly enforced by the U.S. Department of Education, requires parental consent before minors may participate in **surveys**, but only those funded by the Department of Education.

More Information - https://edtech.law/wp-content/uploads/2025/10/three_lies_EdTech_law.pdf