

# Summary of Bill H.4405: Student & Educator Data Privacy

*Please note: This summary was created for the purpose of generating a quick overview and highlights of H.4405. Tool used was ChatGPT.*

## Purpose

The bill strengthens **student and educator data privacy protections** in Massachusetts by regulating how vendors, schools, and the state handle personal information. It creates clear rules for contracts, data security, and penalties for misuse.





---

## Key Provisions

### 1. Definitions & Scope

- **Covered Information** includes personally identifiable information about students, teachers, administrators, or family members (e.g., names, addresses, grades, discipline, health, biometrics, online activity).
  - Applies to **K-12 schools, districts, educational entities, and third-party operators** (vendors providing apps, websites, or online services for school purposes).
- 

### 2. Restrictions on Vendors (“Operators”)

-  **No targeted advertising** to students or staff using school-related data.
  -  **No sale or rental** of student/educator data.
  -  **No profiling** students or educators, unless directly supporting school purposes.
  -  Operators may use **de-identified or aggregated data** for product improvement or research, with restrictions.
- 

### 3. Contract Requirements with Vendors

Every contract with an ed-tech provider must include: - Statement that student data remains **property of the school/district**.

- Explicit ban on using data for advertising or commercial gain.
- Parent/guardian/student rights to review and correct records.
- Strong **security and encryption requirements**.
- Breach notification procedures (must comply with state law).
- Requirement to return or destroy data at the end of contract.

If a contract fails to meet these standards, it is **voidable** and all data must be returned or destroyed.

---

## 4. Oversight & Enforcement

- **Civil remedies:** Students, parents, or districts may sue operators for up to **\$10,000 per violation**, plus punitive damages and attorney's fees.
  - **Commissioner's authority:** Can **bar violators** from accessing student/educator records for at least five years.
  - **Chief Privacy Officer (new role):** Appointed at DESE to oversee policies, training, model contracts, and enforcement.
  - **Board of Ed:** Must set **minimum data security standards** for schools and vendors.
- 

## 5. District Responsibilities

- Develop and maintain a **privacy and security policy**, including breach reporting within **10 business days** to DESE.
  - Designate a **Student Data Manager**.
  - Publish on district websites:
    - Categories of student data collected and why.
    - List of vendors (past 10 years) with access to student data.
  - Provide **annual staff training** on student data privacy (required for educator certification).
- 

## Why It Matters

- Protects **students and educators** from data misuse, breaches, and exploitation.
- Increases **transparency and accountability** for schools and vendors.
- Ensures **families and staff have rights and recourse** if their data is misused.
- Aligns Massachusetts with **national best practices** in student data privacy.