Student and Educator Data Privacy

As artificial intelligence (AI) becomes more integrated into education, ensuring data privacy and security for students and educators is essential. AI-powered tools collect vast amounts of sensitive information, including highly sensitive data, such as student health records, Social Security numbers, and families' credit card data.

Without safeguards, these data can be vulnerable to breaches, misuse, or unethical surveillance. Schools and districts must implement strict data governance policies that comply with federal regulations. Educators should also teach students about digital literacy, emphasizing responsible data sharing and cybersecurity best practices. By protecting data privacy, educators can foster a safe learning environment, build trust in AI technologies, and ensure that AI enhances student learning without compromising individual rights.

Given that AI cannot operate without data—and often, very large amounts of highly sensitive data—the growing prevalence of these tools further exposes education institutions to data privacy and security threats. Education institutions hold unique datasets that include highly sensitive data on both students and their families, making them vulnerable to cybercriminals. Higher education institutions also are more likely than entities in other sectors to pay a ransom.

Due to the vast amount of data available and the lack of coordination among federal agencies and the education community, the education sector has become a target for cybercriminals. One cybersecurity firm estimates that the *minimum* number of U.S. pre-K–12 districts that were impacted by ransomware more than doubled from 45 in 2022 to 108 in 2023.[1] Among the 108 districts, 77 had data stolen, affecting 1,899 schools. Threats against higher education institutions also jumped, from 44 in 2022 to 72 in 2023, with 60 having data stolen. Combining the pre-K–12 and higher education data, the education sector outpaces both health care and government in terms of data security threats. A similar survey conducted worldwide found that an astounding 80 percent of pre-K–12 providers and 79 percent of higher education institutions experienced ransomware attacks, costing millions of dollars in recovery costs.[2]

Transparency is instrumental in protecting students and educators from data harms. To ensure transparency, educators at all levels must be involved in the decision-making process regarding AI vetting, adoption, and deployment. Additionally, school districts and postsecondary institutions should inform students, educators, and families about which AI technologies are implemented, the intended benefits of those tools, the data they require, and the protocols in place to collect, store, and utilize those data. In states with collective bargaining rights, educator contracts should include provisions for data privacy and security.

---

[1] Emsisoft, The State of Ransomware in the U.S.: Report and Statistics 2023 (2024), https://www.emsisoft.com/en/blog/44987/the-state-of-ransomware-inthe-u-s-report-and-statistics-2023/.

[2] Sophos, The State of Ransomware in Education 2023 (2023), https://assets.sophos.com/X24WTUEQ/at/j74v496cfwh4qsvgqhs4pmw/sophos-state-ofransomware-education-2023-wp.pdf.

Considerations for Educators

As AI tools become more common in schools, educators need to consider how these tools are used to protect students' and their own privacy and promote responsible learning environments. You can reduce the risk of data privacy issues and implement AI in a way that aligns with educational goals and values by:

- Understanding student privacy laws (i.e. FERPA, COPPA) and reviewing what data AI tools collect, how it's stored, and who has access;
- Informing students, parents/guardians, and administrators about AI tools being used;
- Implementing secure access controls, such as strong passwords and two-factor authentication;
- Being aware of potential biases in AI algorithms that could impact student outcomes;
- Educating students on the importance of data privacy; and
- Ensuring AI supports, rather than replaces, critical teaching and decision-making processes.

Data Breach Response Checklist for Educators

In the event of a data breach or misuse of information at school, it is critical for educators to respond quickly to protect student and educator privacy. The following checklist provides essential steps to guide you through this process:

1. Report Immediately
    a. Notify school leadership, IT, or data protection officer.
    b. Follow your school or district's breach policy.
2. Contain the Breach
    a. Disconnect affected devices.
    b. Prevent further access to compromised systems or data.
3. Preserve Evidence
    a. Do not delete or modify anything.
    b. Record what happened and when.
4. Document the Incident
    a. What was exposed?
    b. How was it discovered?
    c. Who was informed?
    d. What actions were taken?
5. Support the Investigation
    a. Cooperate with IT and administration.
    b. Provide full, honest information.
6. Communicate Carefully
    a. Only share details if authorized.
    b. Help notify affected individuals.
7. Learn and Improve
    a. Participate in post-incident review.
    b. Suggest or take part in additional training.
8. Follow Laws and Policies

a. Know applicable data laws, such as FERPA.
b. Stick to school policies and legal obligations.