

# FTC Student Privacy “Student Privacy and Ed Tech and P175412” Marsali Hancock

Our children are growing up in the digital culture and environment. That is why it is critical we prepare them with the skills and competencies that they need to succeed. Ideally, educators and parents work together to prepare children to do well and be well using connected devices.

Information gathered from our networks, devices, and applications factor into the algorithms used to create and frame our web experiences. Before a child enters a classroom, schools require a great deal of information about their families. It includes contextual details such as where a child lives, the household income, health and immunization records, Social Security numbers, language spoken at home and cultural and religious background. After enrolling, the information about students continues to grow exponentially.

Artificial intelligence and machine learning make decisions or assist others in making data informed decisions. Data will come from millions of sources and span over the course of a child's lifetime. These sources include data gathered by schools gleaned from devices. This data is vulnerable.

Data left unprotected by schools may potentially negatively impact a child for decades. For example, recruiting companies are hired to identify candidates most likely to succeed in a specific career track or an academic opportunity. Information gleaned from earlier experiences provides insight into the attitudes and behaviors, the emotional and social resilience, and the determination of students. Over the course of a child's learning experience, this data can be rich and deep. Students struggling with some academic subjects, or perhaps personal life challenges such as divorce or behavioral health may be unknowingly excluded and not considered by recruiting companies.

As a society, we understand the value of money and the implication of identity theft financially. However, we do not yet fully understand the value of data and how it drives the digital economy and innovation.

Adult students and parents have little knowledge or control over data shared by schools. Just as parents expect children's physical safety while on campus and traveling on school buses, education organizations are charged with safeguarding students' personal information and education data.

Little information is known about the actual data practices of K-12 schools and districts. However, the state auditor in Missouri (1) recently conducted a series of cyber aware school audits. After she enrolled her own child in school, she recognized the quantity of sensitive personal information about the entire family. As a public institution and data steward, the State Auditor wanted to know how school districts are protecting digital assets. She held schools to the same standards as other public institutions like courts, city government offices, and health departments. Each audit identified significant gaps in basic data protection practices. It finds educators use technology through a consumer lens without training and certification on data governance and compliance. These audits give insight into the current practices of schools in their role as data stewards and articulate the following five most common weaknesses:

1. Data management program- Some districts had not fully established a comprehensive

program or set of processes designed to help ensure sensitive data is formally managed so that student data is available to those that need it while at the same time ensuring individual student privacy is maintained.

2. Account management- Policies and procedures for authorizing, reviewing and removing user access to systems and data were not fully established or documented and employees and staff in some districts were allowed to share user accounts and passwords, or were not required to change their passwords on a regular basis.

3. Security precautions- Some districts did not have an individual appointed to serve as a security administrator or did not have a formal program for offering training or guidance to staff on important data security issues and risks.

4. Incident response planning- Some districts did not have a formal plan or guidelines in place to respond to a data breach or security incident or to promptly resume business functions or computer processing after a disruptive incident.

5. Vendor contracts- In some cases, districts have entered into contracts with third-party vendors to provide technology services, but the contracts were not written in a way that provided information or assurances of the cyber protections that would be taken with information accessible to the vendor. In some cases, districts did not have monitoring processes in place to ensure third-party vendors complied with district security requirements.

Without training it is impossible for an entire generation of teachers and administrators to understand how data is used, its value in the digital economy and innovation, and the implications of unexpected outcomes because of algorithms.

- Without resources, how will schools be able to enforce their own privacy policies or the vendors?
- Can a school comply with COPPA or FERPA if their networks are not secure?
- Do school administrators know what applications or devices are used by school employees and volunteers gathering personal information about students?
- Is it possible for schools to provide notice when they themselves are unaware of the data collected by vendors and other third parties?
- Do schools inventory and classify data gathered by the school, the district, or the applications and vendors they use?
- How can parents be notified of data collected and gathered by commercial entities because a teacher or school official provides permission?

Students and children must rely on others to understand the value of their personally identifiable information and how to protect it. In my own experience enrolling children in school in three states, the Cstar ratings (security rating) for each is far below that of government and industries in the same neighborhood. The school scores range from 278 to 618 with a possible score of 950. Other county websites scored 789. My local bank scored 805.

The most crucial question for the workshop on student and child privacy is how we are going to work together as a nation to protect our children's digital assets, the artifacts of their learning experiences. The school project that used to be taped to my refrigerator door for the family to enjoy is now digitized and potentially commercialized with unknown consequences in our new era of artificial intelligence and machine learning.

Further Resources for The Children's Data Section:

- [Federal Trade Commission - Complying with COPPA FAQ](#)
- [Missouri 2016 Summary of Audit Findings - Cyber Aware School Audits](#)

#### Works Cited

Terlizzi, Gena. "Auditor Galloway Issues Report on Top School Data Security Risks." *Nicole Galloway, CPA*, 9 Nov. 2016, [www.auditor.mo.gov/content/auditor-galloway-issues-report-top-school-data-security-risks](http://www.auditor.mo.gov/content/auditor-galloway-issues-report-top-school-data-security-risks).