



Sep 27, 2018

Categories:

[Publications](#)

Authors:

[Elizabeth J. Reburn](#)

FBI Warns of Cyber Threats to K-12 Students and Unsecured Ed Tech Systems

On September 13, the FBI released a [public service announcement](#) warning of the cyber threats that accompany K-12 schools' rapid adoption and increasing use of education technologies.

Districts use education technologies to compile a vast amount of student data. This far-reaching collection of student data, coupled with the rapid growth and ease of adoption of education technologies by schools, have safety and privacy implications in the event that such data is exploited or compromised. Specifically, the FBI notes that "[m]alicious use of this sensitive data could result in social engineering, bullying, tracking, identity theft, or other means for targeting children." School data breaches are already [wide-spread and frequent](#).

FBI Recommendations

To address these risks, the FBI recommends that parents and families do the following:

- Research existing student and child privacy protections of the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), and state laws as they apply to education technology services.
- Discuss with their local districts about what and how education technology and programs are used in their schools.
- Conduct research on parent coalition and information-sharing organizations which are available online for those looking for support and additional resources.
- Research school-related cyber breaches which can further inform families of student data vulnerabilities.
- Consider credit or identity theft monitoring to check for any fraudulent use of their children's identity.

Conduct regular Internet searches of children's information to help identify the exposure and spread of their information on the Internet.

Action Items

Although the FBI's recommendations are directed to parents and families, school districts should proactively work to address these risks by taking the following precautions:

If you have questions regarding student data privacy or how to work with families to address the risks discussed above, contact [Elizabeth Reburn](#), or any other member of Frost Brown Todd's [Privacy & Data Security Team](#) or [Government Services Practice Group](#).

- Assigning responsibility for student privacy to a specific person or role.
- Creating an inventory of education technology already in use in the district.
- Having a process in place to review an ed tech vendor's privacy practices before use to ensure that the vendor's practices are consistent with the schools' obligations under FERPA, PPRA, COPPA, and other laws applicable to student data.
- Requiring new vendors to sign the district's data security addendum if the vendor's privacy practices are not consistent with the district's compliance obligations.
- Encrypting student data, where possible.
- Being transparent with parents and staff about what technology the school has approved for use.
- Developing and implementing an incident response plan to deal with a data incident or breach.
- Promptly reporting any actual or suspected data breaches to law enforcement.
- Training staff on student data privacy laws. [Good resources](#) already exist.

- Working with parents and families to spread awareness of the known risks and provide resources to families, such as those mentioned in the FBI's recommendations.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.