

How To Protect Student Data Privacy & Security in Education Technology

Webinar Agenda & Discussion Topics

Overview

How many new apps and/or vendors has your district adopted in the past 2 years? You might be surprised to learn that number is actually much higher than you think. The EdTech industry is exploding. Though these tools can provide many benefits, they are also creating real student privacy concerns and data security risks.

During this webinar, we were joined by Marlo Gaddis, Chief Technology Officer at Wake County Public Schools, and Libbi Garrett, Director of Resource Programs at CITE (California IT in Education), to discuss the benefits and challenges of managing student data privacy and security in the context of education technology.

Time	Detail
2 mins	Opening remarks, housekeeping, agenda
5 mins	Introduction: There is no data privacy w/o data security
~5 mins	Panelists Introduction/Background
30 mins	<p>Discussion Questions/Topics</p> <ol style="list-style-type: none">1. California and North Carolina, along with many other states, have passed student data privacy and data security laws over the past several years. Why are these laws needed in addition to federal regulations like FERPA, COPPA, CIPA, etc?2. How has the use of education technology (3rd party apps) changed or evolved over the past few years, and how are you seeing that impacting student data privacy and security?3. Third party applications can be a popular and valuable tool for educators, do you have any tips on how to vet this type of resource?4. What steps can districts take to make sure they are sharing student data with vendors in a way that is secure and compliant?5. What would you like other district technology and/or administration leaders to understand about how data security impacts data privacy and compliance with federal and, in many cases, state regulations?
15 mins	Audience Q&A
3 mins	Conclusion & Call To Action



Managed Methods

Cloud Security Made Easy

Monitor, Audit & Control Cloud Risks — Made Easy!

ManagedMethods makes Google Workspace and Microsoft 365 cybersecurity, student safety, and compliance easy for K-12 school districts—no proxy, no agent, no extension, and no special training needed.



Monitor & Audit

Automated security & behavior monitoring & remediation 24/7/365 with simple reporting



Cyber Safety

Detect self-harm, cyberbullying, abuse, discrimination & explicit content signals



Data Security

Data loss prevention for sensitive student, staff, & district data stored in Google Workspace & Microsoft 365



Threat Protection

Stop phishing & malware attacks in Google Workspace & Microsoft 365 email, files & drives