



# Cyber Safety & Data Security Compliance for K-12 Schools

## Regulatory Compliance for Schools using Google Workspace for Education & Microsoft 365

Meeting federal and state compliance regulations is a challenge for K-12 IT teams. Compliance visibility and control is lost when their district moves to cloud data storage and communications.

### Close cyber safety and data security compliance gaps in your district's cloud environment

If your schools are using Google Workspace for Education or Microsoft 365 without a cloud monitoring tool you're vulnerable to cyber attacks and compliance gaps.

#### Federal Regulatory Compliance for K-12 Schools

- Health Insurance Portability and Accountability Act (HIPAA)
- Children's Internet Protection Act (CIPA)
- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Rule (COPPA)
- Federal Tax Information (FTI) compliance
- Civil Rights Act

#### Benefits

- Easy to use, fast implementation
- Out-of-the-box and customizable compliance auditing and reporting
- Compliance, safety, and security monitoring on any device, from any location
- Gain visibility into data access and use in Google Workspace and Microsoft 365
- Detect discriminatory, explicit, and other harmful content in text and images in Gmail, Google Docs, Chat, and more
- Top-rated customer tech support

ManagedMethods' cybersecurity and safety solution provided us a level of visibility we needed to ensure the security and safety of our students and staff. The platform was quick to deploy and gave us immediate insights."

*Steamboat Springs School District*



#### Data Security

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



#### Threat Protection

Detect phishing & malware attacks in Google Workspace & Microsoft 365 email & drives



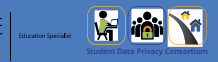
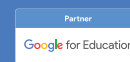
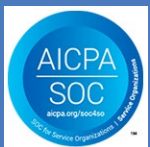
#### Monitor & Audit

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



#### Safety Signals

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





## Committed to Student Data Privacy

ManagedMethods does not store or access your staff and student data except when authorized by you in the context of a support ticket. All support access is logged and tracked. The entire ManagedMethods support team is background checked.

## Where Are Your Security & Compliance Gaps?

Features & Functions	Managed Methods	Content Filter	Campus Safety Management
FERPA, COPPA & CIPA compliance	●	●	
100% cloud-based technology protect data in any location, on any device via application account login	●		
APIs scan images & content in emails, files, and chat	●		
Detect & control explicit, harmful, and violent content in school Google Workspace & Microsoft 365 accounts	●		
Protect against phishing, malware & ransomware	●		
Automate data loss prevention with policy enforcement	●		
Detect account takeovers by login & behavior activity	●		
Approve and unapprove account logins by location	●		
Automate data security compliance reporting	●		
Account audit & lock for compliance issues	●		
Detection of 3rd party SaaS apps with risk rating & control	●		
Identify explicit images & content, cyberbullying, self-harm, discrimination, threats of violence in Google & Microsoft 365	●		●
Google Meet auditing & reporting	●		
Google Chat safety, data loss prevention, & CIPA monitoring	●		
Keyword & regular expression content monitoring	●	●	
AI & machine learning powered content monitoring	●	●	
Browser-based technology, security based on device (must have proxy, agent, or extension installed on device)		●	
Chrome extensions detection & management		●	
Protect students from visiting websites that curate explicit, harmful, and violent content		●	
Prevent students from wasting time online when they should be focused on school work		●	
Identify cyberbullying & threats of violence on social media			●
Anonymous student tip line			●
Message & file archiving for litigation holds			●
Professional safety team to analyze & report alerts (Gaggle & Securly only)			●

## Committed to Student Data Security & Privacy

ManagedMethods does not store or access your staff and student data except when authorized by you in the context of a support ticket. All support access is logged and tracked.

The entire ManagedMethods support team is background checked.



## Data Security & Compliance

- Discover and act on suspicious logins from unapproved locations
- Discover personally identifiable information, credit cards and other financial information being shared with outside the organization
- Detect and act on emails with phishing links
- Revoke excessive sharing of confidential information outside of the district
- Remove risky 3rd party apps with access to organizational emails and data

## Cyber Safety Signals

- Discover student self-harm behavior in emails, documents, and images
- Identify text that may be indicative of bullying, racism, violence, and other troublesome behavior
- Assign roles-based notifications of student behavior risks to school principals and psychologists for intervention

## Securing Over 1,000,000 Accounts in K-12

“You’re going to remember a time before you had ManagedMethods, and then you are going to appreciate how good and useful it is now. If you don’t have a CASB, you definitely need to invest in one and I recommend that you invest in ManagedMethods.”

Cody Walker  
Director of Technology  
West Rusk CCISD, TX

“The student safety component of ManagedMethods paid for itself within a few weeks. We had a couple of incidents that we would not have caught had it not been for ManagedMethods. It’s effective and within a few clicks I can see exactly what’s happening across my Google Workspace infrastructure.”

Neal Richardson  
Director of Technology  
Hillsboro-Deering School District, NH