K-12 BLUEPRINT

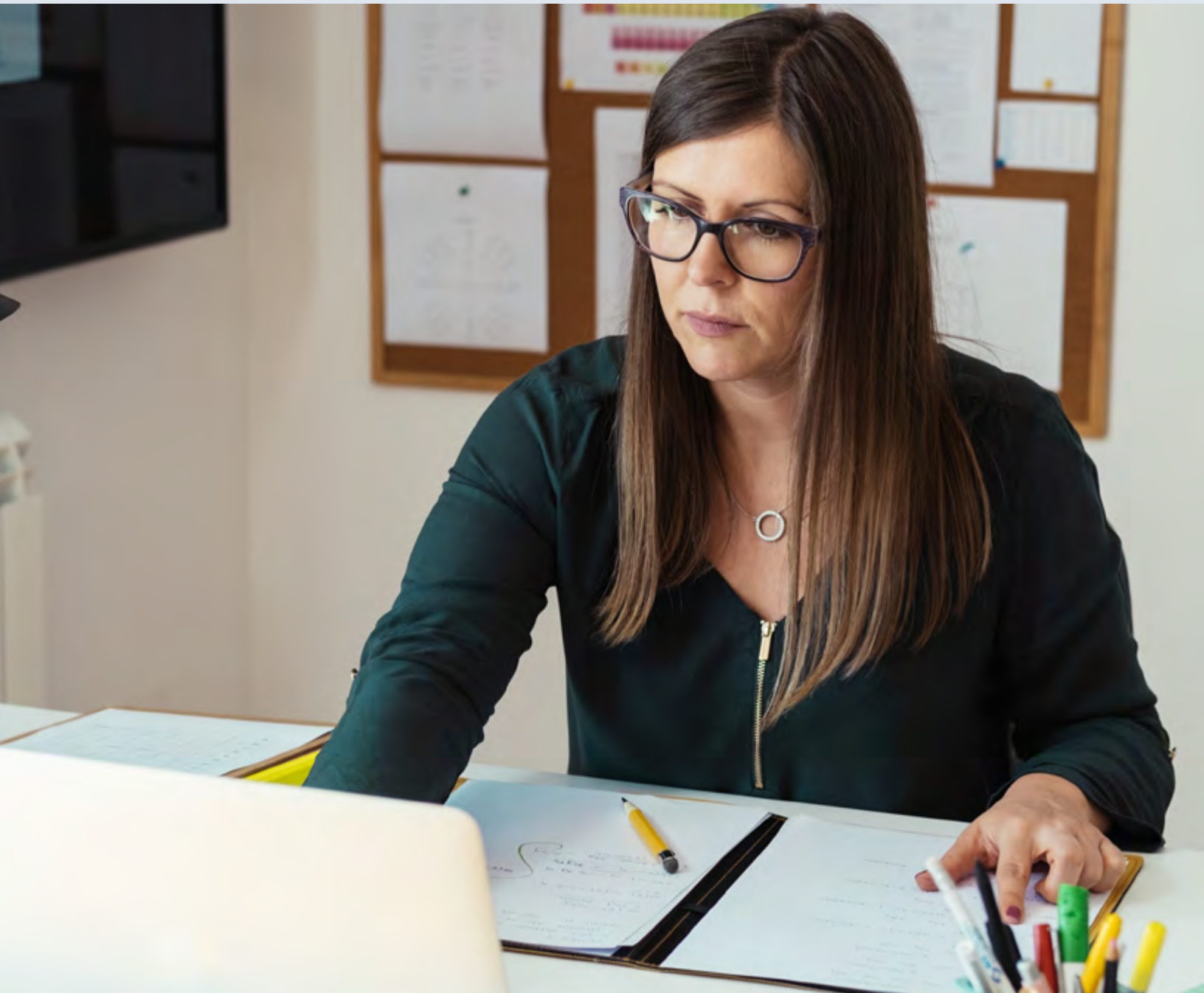
Security Solutions Guide | Sponsored by Microsoft

April 2023 | Prepared by Clarity Innovations, Inc.

DATA DILEMMAS

Information Governance and Electronic Discovery in K-12 Education

Understand how Microsoft Purview eDiscovery effectively preserves and analyzes critical data during cyber investigations and legal holds.



Executive summary

School districts face a multitude of challenging threats and hazards, including human-caused cyber incidents. Reported cyber incidents and data breaches in schools rose from 400 in 2018 to over 1,300 incidents in 2021.[01]

From 2016 to 2020, staff were responsible for most accidental data breaches and students accounted for most of the intentional breaches. Whether deliberate or accidental, these incidents can disrupt educational operations, expose personally identifiable information (PII), and lead to hefty recovery costs, generating an extreme need for enhanced information governance and electronic discovery processes.[02]

The Cybersecurity and Infrastructure Security Agency (CISA) recommends that all school districts develop and exercise a cyber incident response plan.[03] Response plans should include what needs to be done before, during, and after a cyber incident. School administrators must be able to freeze, archive, and access electronically stored information (ESI) in order to comply with amendment 37(e) in the Federal Rule of Civil Procedure, which requires organizations to preserve ESI in the event of a triggering event for reporting requirements and litigation.[04] K-12 organizations can use tools in conjunction with information governance and electronic discovery processes, like the Electronic Discovery Reference Model (EDRM) model, to combat these types of incidents.[05]

To combat cyber incidents, school districts need tools to:

- Monitor critical changes to accounts and policies
- Track applications and users on a device
- Audit trails of Active Directory Domain Services
- Implement security policy
- Control privileged use of systemwide resources

Microsoft Purview eDiscovery (Premium)* delivers an end-to-end workflow to identify, preserve, collect, process, review, analyze, and export content for internal and external investigations, such as cyberbullying, oversharing of sensitive data or content, and sharing of inappropriate data or content.[06] This tool enables administrators to identify people of interest and analyze their data in an efficient manner. Schools are also able to create litigation holds that preserve and retain mailbox content for all users in an organization.[07]

In comparison, Google Vault*, an archiving and compliance solution used for information governance and ediscovery, is only able to identify, preserve, and collect data. This tool aims to keep data safe from accidental or intentional deletion to ensure compliance with educational IT standards and legal investigations. However, data needs to be exported for further analysis and review.[08] Microsoft's all-in-one solution reduces the number of tools that schools need to investigate threats and develop information governance and electronic discovery processes.

Identifying potential risks to school districts

Since many students and staff often generate the most risk when it comes to potential cyber incidents, it is imperative that schools are able to quickly flag sensitive content before cyber incidents occur. Schools can use eDiscovery to efficiently search for content using machine learning in emails, instant messages, files, and even within third-party platforms like Canvas* to identify incidents of cyberbullying or inappropriate distribution of data or content.

Machine learning processes like deep indexing, email threading, and near duplicate detection reduce large data sets into manageable collections. Smart tags and technology assisted review tools in eDiscovery also support machine learning to refine and identify relevant data.

Google Vault, on the other hand, uses simple search queries and Boolean operators to find data.[09] This makes identifying relevant data slower and requires users to identify potential risks before they occur.

Schools can take their information governance tools a step further with Microsoft Syntax*. Syntax allows IT staff to efficiently capture, classify, audit, and flag documents and forms that require additional risk mitigation. Using "intelligent document processing, content artificial intelligence (AI), and advanced machine learning", it can provide schools yet another way to reduce risk and maintain compliance while accurately and consistently searching, managing, and controlling data and content.

Extending data collection across tools

Microsoft Purview eDiscovery (Premium) goes beyond simplifying data discovery within popular Microsoft tools like Teams for Education*, SharePoint*, OneDrive*, and Exchange Online*.

Schools can also:

- Reconstruct Teams conversations
- Collect cloud-based links and attachments in email and Teams
- Run queries across hundreds of non-Microsoft 365 file types
- Collect data from third-party sources like Facebook, Slack, and Zoom[10]

With Google Vault, data discovery and retention are limited to Google services like Gmail*, Google Drive*, and Google Chat*.[11] It does not connect to third-party applications or services.

Collecting relevant data for potential litigation

After identifying potential risks, data must be collected for further use in the e-discovery process and school investigations. eDiscovery allows schools to isolate data at the source so that IT departments can maintain existing Microsoft 365 security and compliance boundaries. This keeps IT administrators from having to go back to the source to find missing content or create duplicate data to preserve records. Rather, they can search for and collect live data that is relevant to their investigation.

Alternatively, Google Vault uses a search and export process that requires data to be copied or downloaded. This requires IT administrators to utilize static data sets that may not include the most current or relevant data, depending on the search parameters and date it was exported. When static data sets are used in the collection process, IT administrators often need to preserve duplicates or large volumes of data and critical information.

Preserving critical data from alteration or destruction

Government employees like educators and school district administrators are subject to Freedom of Information Act (FOIA) requests. Under this statute, school districts must disclose communication like email messages or chats upon request. K-12 organizations need ways to quickly gather relevant communication from any type of user account in the event of a disclosure request.

eDiscovery allows IT administrators to place legal holds on several data sources that are associated with specific users. Microsoft Litigation Hold* takes data preservation a step further by giving administrators the ability to retain all Exchange mailbox content including deleted items, original versions of modified items, and archives.[12] Litigation Holds can remain in place for a specified period of time or last indefinitely, and storage quotas are increased to ensure all communication is saved, making it effective for gathering information needed for disclosure requests.

While Google Vault can hold active and deleted messages and drafts in response to an investigation or disclosure request, it does not preserve linked files, discarded drafts, or messages sent from other Google services, like Google Calendar* or Google Docs*, unless comprehensive message storage is activated.[13] IT administrators can also create retention rules that apply to all users or groups in an organization to control how long data is preserved.[14]

Comparison of stages included for electronic discovery

EDRM Stages	Microsoft Purview eDiscovery (Premium)	Google Vault
Identification	👍	👍
Preservation	👍	👍
Collection	👍	👍
Processing	👍	👎
Review	👍	👎
Analysis	👍	👎
Production	👍	👎
Presentation	👍	👎

Conclusion

K-12 schools need to be able to respond to cyber-incidents, investigate activities across a range of applications, and collect relevant data that pertains to investigations and requests. Tools like Microsoft Purview eDiscovery (Premium) and Google Vault provide schools with solutions to investigate cyberbullying and threats that arise from oversharing or inappropriate sharing of data or content in emails and chats and develop information governance and electronic discovery processes. While Google Vault allows IT administrators to conduct the identification, collection, and preservation stages of electronic discovery processes, eDiscovery allows IT administrators to run through all stages of traditional electronic discovery to fully conduct cyber investigations.

Rather than using separate tools, Microsoft's all-in-one solution allows IT administrators to continue their electronic discovery by processing relevant investigation data for further review, running additional queries to reduce data volume, annotating and tagging specific documents, and using integrated analytics tools to further cull data and organize content. When the data is ready to present, Microsoft allows users to export documents for legal review. By utilizing eDiscovery across school IT infrastructure, schools are able to implement CISA's recommendation to develop a cyber response plan. For these reasons, Microsoft Purview eDiscovery (Premium) is the ideal choice for K-12 schools.

Side-by-side comparison

Features	Microsoft Purview eDiscovery (Premium)[15]	Google Vault[16]
Cost	Included in select Microsoft 365 subscriptions, including Education A5	Included for users with Google Workspace license and Vault license *Note: Vault licenses are included with all education editions.*
Data Connections	Microsoft solutions and over 60 third-party connectors	Google services only
Data Analytics Method	Machine learning with smart tags and technology assisted review tools	Search queries and Boolean operators

Sources

01 CISA: 2023 Protecting Our Future
02 U.S. Government Accountability Office: Data Security
03 CISA: 2023 Protecting Our Future
04 American Bar Association: ESI Spoliation Sanctions
05 EDRM Model
06 Microsoft: Overview of Microsoft Purview eDiscovery (Premium)
07 Microsoft: Create a Litigation Hold
08 Google Vault
09 Google: Get started with Vault search and export
10 Microsoft: Learn about connectors for third-party data
11 Google: Supported services and data types
12 Microsoft: Create a Litigation hold
13 Google: Place Gmail messages on hold
14 Google: What's the difference between a hold and a retention rule?
15 Microsoft: Microsoft Purview eDiscovery solutions
16 Google: Google Vault