Securing Data in Google Apps for Education: K-12 Schools

Auditing & Compliance

- **FERPA - Family Education Rights & Privacy Act**
- **CIPA - Children’s Internet Protection Act**

How Tos

- **How To Report on Collaboration and Adoption of Google Apps in K-12 Schools**
- **How To Discover, Classify, Remediate, and Monitor 3rd Party Apps in Google Apps in K-12 Schools**
- **How To Effectively Monitor Student Documents in Google Docs, Sites, and Google Drive**
- **How to Change Ownership of Externally Owned Google Docs**
- **How to Remove Public Exposure in Google Docs and Sites**
- **How To Transfer Data Ownership In Google Docs**

Case Studies

- **Teach for America**
- **Mattawan Consolidated School**
- **Edina Public Schools**
- **Escondido Charter School District**
FERPA is a federal law that protects the privacy of student education records.

The act has 2 main aspects:

- Providing students (or parents) with access to their educational data
- Privacy policy – protect and privacy of the student’s education records

Challenge: The same FERPA guidelines apply to data stored in the cloud - maintaining adequate access controls to ensure that student records are not exposed.

<table>
<thead>
<tr>
<th>Action Required</th>
<th>CloudLock Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure access to student sensitive data</td>
<td>CloudLock Apps Firewall discovers all 3rd party applications and their access rights and lets the domain administrators remediate and revoke access for unapproved applications.</td>
</tr>
<tr>
<td>Find all documents containing student PII</td>
<td>Compliance Scan – lets you find files containing student Personally Identifiable Information (PII).</td>
</tr>
<tr>
<td>Ongoing monitoring and alerting</td>
<td>Security Policy Engine lets IT set content, context and sharing based policies and put security monitoring on autopilot. The policy engine alerts designated security staff when sharing policies on student documents do not follow acceptable use policies.</td>
</tr>
<tr>
<td>Correct access rights</td>
<td>Fix the access right on individual files or in bulk</td>
</tr>
<tr>
<td>Auditing</td>
<td>Full audit of all documents in the domain and their access rights</td>
</tr>
</tbody>
</table>

Auditing & Compliance: CIPA - Children’s Internet Protection Act

Federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers.

Specifically:

- Protect minors’ private information from leaking to un-authorized individuals
- Restrict minors’ access to materials harmful to them and protect them from exposure to content that is not appropriate

Challenge: Ensure that minor are not exposed to harmful content via Google Docs and Sites

<table>
<thead>
<tr>
<th>Action Required</th>
<th>CloudLock Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover and revoke unapproved 3rd party apps</td>
<td>CloudLock Apps Firewall discovers all 3rd party applications and gives the domain administrators the tools they need to ensure students are not subjected to obscene content. They can then take action and revoke the unapproved applications from the domain.</td>
</tr>
<tr>
<td>Find harmful content</td>
<td>CloudLock provides a robust content and keyword search on all documents in the domain. Detect obscene content, bullying etc. Security Policy Engine lets you set content, context and sharing based policies and put security monitoring on autopilot.</td>
</tr>
<tr>
<td>Stay on top of external sharing</td>
<td>This is supported by automatic discovery of all documents and users in the domain and classification of documents by access and exposure level and external sharing</td>
</tr>
<tr>
<td>Detect and protect all personal records</td>
<td>Compliance Scan provides the ability to effectively find and flag files containing student Personally Identifiable Information (PII).</td>
</tr>
</tbody>
</table>
How To: Report on Collaboration and Adoption of Google Apps in K-12 Schools

Use Case: K-12 schools piloting or moving to Google Apps for Education need to understand adoption of the online productivity and collaboration suite, and need to understand how students and teachers are collaborating.

Collaboration is quickly changing the landscape of K-12 schools, as it becomes one of the major pillars of academic success. Collaboration is happening amongst students when they are working on school projects, and with teachers, with a feedback mechanism directly within Google Docs.

→ Click here for more about the collaboration benefits of Google Apps for Education.

With the introduction of Google Docs, students are now empowered to not only create documents but also share them. The role of IT has transitioned from an infrastructure provider that frames and limits collaboration into predefined boundaries, into facilitators of collaboration. With that said, every school still needs to make sure that collaboration practices align with school policies and regulations to foster safe collaboration for minors.

In this How To we will briefly discuss how IT administrators at schools using Google Apps for Education can monitor and report on student collaboration and the adoption of Google Docs, Sites, and Drive.

Step #1 – Understand Who is Using Google Docs, Sites, and Drive

This step is necessary especially for schools that are early in the adoption cycle. It is important to understand how both teachers and students are actually using the tools they have been given.

CloudLock’s user view gives a breakdown of Google Docs users by most active to light users. From this view, a simple drill-down lists all users.

This review gives an overview of the overall adoption and usage of Google Docs by teachers and students, and a tool to identify whether additional training or workshops are needed in order to ensure adoption.
Step #2 – Understand How Google Docs Are Being Shared

It is important to understand how Google documents are being shared to answer:

- Are students sharing documents externally?
- Is anyone external to the school sharing documents with students?
- What is the nature of these documents?

From this view you can drill-down to get a full list of collaborators for each document allowing you to inspect document content and make sure it is not in violation of any school regulations or policies.

Step #3 – Set Policies to Monitor Student Sharing

Put security and monitoring on autopilot by creating school-specific policies using CloudLock’s Policy Engine. The policies can identify and alert on violations based on:

- Ownership criteria – Alerts for specific owners
- Sharing rules – Set rules stating who can and cannot share with whom
- Content criteria – Find content that is inappropriate for students
How To: Discover, Classify, Remediate and Monitor 3rd Party Apps in Google Apps for K-12 Schools

Use Case: K-12 schools piloting or moving to Google Apps for Education need to understand why they must monitor 3rd party apps that have been granted access to the domain and how 3rd party apps should be monitored and controlled.

The adoption of Google Apps among students and teachers in K-12 schools has provided easy collaboration on papers and reports as well as streamlined IT operations and incredible cost savings.

While the implementation of Google Apps for K-12 vary from one school to another (some schools organize teachers, staff, and students by Organizational Unit, others use Groups, while still others use separate domains), all schools must comply with regulations like FERPA and CIPA, protecting private student information and ensuring that minors are not exposed to inappropriate content.

While our CloudLock for K-12 Education section covers How To Effectively Monitor Student Documents in Google Docs, Sites, and Google Drive as well as FERPA and CIPA compliance, the following guide expands the discussion to 3rd party apps to:

• Explain why K-12 schools must monitor 3rd party apps that have been granted access to the domain
• Review the process in which 3rd party apps should be monitored and controlled

What Are 3rd Party Apps and Why Should We Care?

3rd party applications extend the functionality of the Google Apps platform and can provide significant value. However, schools need to control which 3rd party apps can be granted access to the environment by teachers, students, and admins.

When a user provides a 3rd party app with their Google Apps credentials, the app is granted access to the domain, and is given access to that user’s data like email, docs, calendar, and contacts.

While many 3rd party apps require these credentials, the sheer volume of users and web apps creates risk, with some apps requiring excessive access rights (including access to all documents in the domain) and others subjecting students to questionable content.

The Problem

Although the access required by 3rd party apps may very well be legitimate to ensure expected behavior, they also open a backdoor into the domain. This creates exposure for end users and the school’s domain, which can be exploited by these applications as well as by the privileged users of the vendors behind them.

Despite the fact that end users can give third party web and mobile apps access to sensitive data in Google Apps, the IT department is still charged with reviewing app security and maintaining the school’s Approved Applications Policy (AAP).

Control The Information 3rd Party Apps Can Access

CloudLock Apps Firewall helps K-12 schools extend their security practices to include apps that have been granted access to their Google Apps domain. It discovers all apps installed by end users (including students) and shows the extent of permissions and access available to each installed application.

The following 4-step process lets schools implement a proactive approach to cloud application security in Google Apps:
Step #1 – Discover

Automatically detect all apps granted access in the domain. CloudLock Apps Firewall lists all the applications granted access to your domain. Once all applications are discovered you can:

- View all applications with access to the domain
- View all teachers/students/admins that have granted access to a specific application
- View all applications that a specific user has added

Step #2 – Classify

Allow or ban applications based on their risk profile. To review the risk profile for each application:

- Check the scope of each application, the resources it has been granted access to, and the extent of the access rights granted to each application
- Understand what each application does
- Review the vendor profile for each application – Is it a trusted and known entity that has passed security and other audit certifications?
- See who has granted access to this application: how many users, whether the app has been added by domain administrators (privileged domain users) or regular domain users.
Step #3 – RemEDIATE

Take action to secure your domain by revoking unapproved apps and notifying associated teachers and students. CloudLock Apps Firewall provides effective remediation of potential security challenges when you discover applications that should not be granted access to the domain. In these cases you can take one of the following actions:

- Notify users of unapproved apps – Notify a single user or all users that have granted access to selected apps
- Revoke the application(s) – This measure can be used for risky applications that pose a significant security threat to the organization and need to be removed from the domain immediately. Select the app(s) to be revoked and choose <Revoke Application>
- Periodically check that Banned applications have not been added back into the domain.

![Image of CloudLock Apps Firewall interface](image)

Step #4 – Monitor

Continuously monitor the environment for new apps that are added to the domain and repeat steps 1-3. CloudLock Apps Firewall provides ongoing monitoring and discovery of new applications granted access to your domain as well as the ability to monitor user adoption.

Conclusion

CloudLock Apps Firewall lets K-12 schools effectively discover, classify, remediate, and continuously monitor Google Apps domains for 3rd party applications that have been granted access, giving schools a proactive approach to ensure ongoing compliance with FERPA and CIPA.
Use Case: Administrators need the ability to gain “view” access to student documents in a non-disruptive way. Currently, the administrator must change the student’s password and log in as that student. This approach is manual and time consuming, and results in multiple password changes for each incident.

Google Apps for Education provides schools with an unmatched set of tools, allowing students and teachers to collaborate in ways that were impossible just a few years ago. The adoption of Google Docs in K-12 schools enables students to collaborate amongst themselves when they are working on school projects, and with teachers, with a feedback mechanism directly within Google Docs. Submitting work can be accomplished by simply placing a document in a collection or folder that is specially marked to indicate submitted work, supporting a paperless and green process.

When looking at the collaboration, cost benefits (Google Apps for EDU is free), and ease of use, adoption of Google Apps is a no-brainer. So… is there a catch? No. No catch.

But… the introduction of any new system brings new challenges with it. Because K-12 schools need to track and monitor student activities, they need to be able to effectively monitor the content of students’ Google Docs to guarantee that new assets follow all rules and regulations.

In this How To we will discuss 4 simple steps to monitor student activities in Google Documents, Drive and Sites.

Step #1 – Review Violations of Default Policies

In most k-12 schools, students only collaborate with other students and teachers using Google Docs. Documents shared externally or from the outside in should be monitored to ensure they are not shared with the “wrong” people and that they do not contain prohibited content.

Start by reviewing CloudLock’s default policies as they are available from the dashboard:

1. Review Public sharing set on documents owned or collaborated on by students
2. Review External sharing set on student owned documents
3. Inspect externally owned documents shared with students

You can do this directly from the CloudLock dashboard by clicking on the exposure links and external documents.

You can also select individual students and inspect the sharing settings on all their documents.
Step #2 – Create and Review Customized Content Policies

CloudLock’s policy engine allows you to create content specific policies to flag documents based on metadata and content. Content specific policies let you detect documents that contain information that should not be accessible to students.

For more information, see the following resources:

- How to Enable Secure Collaboration for Google Docs and Sites with CloudLock’s Security Policy Engine
- How to Protect Intellectual Property in Google Docs, Sites and Drive

You can get alerts on specific policy violations or any new document exposures. This will give you an effective way to only review documents that violate specific policies or become exposed.

Step #3 – Inspect Suspicious Documents

Once you’ve been alerted to specific documents that violate a policy (default or custom), you’ll want to inspect its contents to validate the severity of the violation. This simple task becomes an operational challenge when there are hundreds or thousands of student documents that need to be inspected.

CloudLock provides domain administrators an easy way to inspect content in student documents:

1. Find the document you want to inspect
2. Review the document owner, collaborators, and recent changes
3. Click on the “View Document” button to gain access to the document in a non-disruptive and time efficient manner

Note: This action will be audited in a tamper-proof audit log
Step #4 – Invoke Bulk Operations

Once you identify documents that were either shared incorrectly, violate the school’s sharing policies, or contain sensitive content that violates compliance regulations, you can change and correct permissions or lock the files to use as evidence.

CloudLock’s bulk operations allow you to select some or all of the identified documents and perform the following functions:

1. Add or remove collaborators
2. Change collaborator access rights on some or all documents in the domain
3. Copy files and transfer ownership

In summary, monitoring student activities to ensure that content is appropriate and documents are shared properly is a fundamental and necessary responsibility for every K-12 school to comply with regulations and ensure student safety.

CloudLock gives domain administrators the tools necessary to perform these tasks effectively while letting students and teachers fully enjoy the collaboration benefits of using Google Apps for Education.
How To: Change Ownership of Externally Owned Google Docs

We often hear our customers ask “How do I change ownership of externally owned Google Documents and prevent the loss of intellectual property?”

We’ll show the steps to take to change ownership of Google Docs that are owned by an account outside your company’s domain. Since only a document owner can change permissions, this tutorial shows how to create a copy of an externally owned document, assume ownership, and set sharing permissions.

First, let’s understand the source of these requests. Here are some examples:

- Employees using their personal Gmail accounts to create documents for work – This often happens in a company’s early implementation stage, where users do not distinguish between domain accounts and their personal Gmail accounts and use them interchangeably.
- External partners or third party vendors create documents and assets for your company – Even though these assets are your IP, technically they are the “owners” of these assets within the Google Apps account framework.

Why is this a problem?

If a document is owned by a non-domain user (i.e. a private Gmail account or a user from a different domain) you cannot assume ownership of this document even if you are a collaborator.

These cases pose a risk of data leakage or loss if the external owner deletes the document mistakenly (or maliciously in some cases) or deletes the account and loses all their documents.

The Solution

Using CloudLock’s bulk copy feature is an effective and secure solution to changing ownership of externally owned Google Documents. Here is how it works:

Step #1 – Find the Documents You Need to Copy

Perform a keyword search to find all the relevant documents. CloudLock’s advanced search capability allows you to search your entire domain for documents by any attribute (names, owners, shared with, type, exposure etc.).

Or use the summary on the dashboard to easily get all the externally owned documents:
Step #2 – Select the Documents and Copy them in Bulk:

- Choose some or all of the documents you would like to copy
- Choose the “Copy Documents” option from the “More Actions” menu (see below)
- Designate a new owner (the person in your company that should own the documents)
- Specify the collection into which these documents should be placed

Step #3 – Perform an Audit

All operations performed by CloudLock (including the operations that are done in bulk on a selection of documents) are recorded and saved in a tamper-proof audit log.

Some key benefits of using CloudLock’s copy function:

- Performing a keyword search by owners gives you a quick way to find and select documents
- You can perform this operation in bulk on several documents
- Documents never leave Google Docs
- This is a fully automated operation that runs in batch mode
- It gives the flexibility to choose if permissions of the original document(s) will be preserved or removed when copied
- You are able to copy the files to a designated collection
- All actions are audited
How To: Remove Public Exposure in Google Docs and Sites

Data breaches, whether they happen mistakenly or maliciously, should be addressed and corrected immediately to minimize any possible damage to the organization as a result of this exposure.

CloudLock gives you the tools you need to find public exposures, remove them to secure sensitive documents and sites and continuously monitor your domain to make sure you stay on top any new exposures.

This is how CloudLock can help you take the necessary steps to secure you Google Documents and Sites.

Removing Public Exposure in Google Docs

Step #1 – Find Sensitive Documents

Perform a keyword search to find all the sensitive documents. CloudLock’s advanced search capability allows you to search your entire domain for documents by any attribute (names, owners, shared with, type, exposure etc.).

Step #2 – Sort to find which of the Sensitive Documents are Publically Exposed

At this point you can also export the list of results, showing potentially sensitive documents that are exposed.
Step #3 – Audit the Documents

Verify that you do not have false positives or vise versa. Examining the document contents is available for privileged users, and gives you the ability to verify that documents should be secured.

Step #4 – Select Documents

Choose the documents you would like to secure, and remove the public exposure by selecting this operation from the drop down list.

Step #5 – Monitor your Google Documents

To make sure no new exposures are created. Every time a new exposure is created you will get an email alert.
Removing Public Exposure in Google Sites

Step #1 – Find Exposed Sites

CloudLock’s dashboard gives you an audit of all Google Sites that are exposed publicly (visible to anyone on the internet) or externally (visible to users outside of your domain).

Step #2 – Examine Content in your Google Sites and Remove Exposures

Change permissions on Sites that should not be publicly or externally shared.
How To: Transfer Data Ownership In Google Docs

When a Google Apps domain administrator deletes a user account, the documents owned by that user get deleted automatically. Basic ownership transfer functionality is available through the Google Apps control panel, however most companies need extended capabilities.

How Transferring Google Docs Ownership Is Different With CloudLock

CloudLock expands upon the included document transfer features in Google Apps, adding:

- **Any Domain User Can Transfer Ownership** – Google’s built-in tool only allows domain super admins to transfer ownership of documents. With CloudLock, any user can be given ownership transfer rights.
- **Interactive Mode** – CloudLock’s transfer ownership functionality provides a visual wizard that guides you through advanced data migration options
- **Audit Trail** – CloudLock logs which files where migrated, when, by and to whom, and whether the original owner still has access rights; a feature that is mandatory for companies using Google Apps in a regulated environment
- **Transfer to a Designated Folder** – Rather than simply dumping all files, CloudLock transfers files to a designated folder, helping to organize data on the target user’s environment
- **Control Access Rights of the Original Owner** – In some cases, companies want to transfer ownership of a user’s documents, but want the original owner to retain access. With CloudLock, transferring ownership has granular access options for the original user
- **Support for Collections** – CloudLock’s transfer ownership functionality lets you maintain the same collection (folder) structure, keeping documents organized
Collaboration Security Case Study

Teach For America Uses CloudLock to Increase Operational Efficiency

At a Glance

Industry: Not for Profit
Number of Employees: 2300

Drivers for Google Collaboration:

- Increased speed and ease of collaboration among first-year teachers across the country
- Quick auditing capabilities to ensure that documents and sites remain secure from one year to the next

Requirements for Secure Collaboration

- Comprehensive insight into user adoption and document control/visibility

Consequences for Not Implementing Security Controls:

- Elevated risk of exposing sensitive information via public sharing
- No avenue for administrators to monitor content added, edited and shared in documents and sites

Primary CloudLock Collaboration Security for Google Apps Features Used:

- Security Policy Engine to create, manage and enforce Acceptable Use Policies
- Bulk Operations to increase efficiency in auditing documents and removing exposures

The Organization

Teach For America is the national corps of top college graduates and professionals who commit to teach for two years in urban and rural public schools and become lifelong leaders in the effort to expand educational opportunity.

Teach For America’s network for the 2012-13 school year includes more than 10,000 teachers in 46 regions across the country, and nearly 28,000 alumni working in education and many other sectors to create the systemic changes that will help end educational inequity.

The Challenge

After approximately 30 hours of independent work and observation of experienced teachers, corps members attend an intensive five-week training institute and a regional orientation to the schools and communities in which they will be teaching.

During the intensive summer training program, 5,800 first-year teachers need to collaborate, do homework, and access documents anywhere, anytime, and the challenge has been sharing documents externally during this training time. Although Teach For America has a limited number of laptops and workstations, most teachers choose to bring their own device to the summer training program, thus requiring the team to find another solution that is secure and yet externally shareable and accessible. Google Apps allowed Teach For America to collaborate in real-time across the country, enabling more seamless training and on-boarding of teachers during the intensive summer training time.

After the summer training institute and every year when staff transition, Teach For America needs to audit hundreds accounts to make sure that documents and sites remain secure.

“It takes too much time to figure out how many documents and sites we have, which users are gone, and who has access. We turned to Google, and they recommended CloudLock to us.”

— Patti Santacroce, Managing Director of Application Administration and Support
Teach For America
Preventing Data Leakage In Google Apps

CloudLock gives Teach For America an effective process to secure sensitive data like donor and corps member information with the following capabilities:

- Bulk operations for permissions changes, removing internal and external exposures
- Transfer Ownership with a full audit log of all the actions
- Exposure Notifications

Saving Time and Adding Security

With CloudLock, Teach For America is able to automate manual processes to spend more time on strategic projects. “Without CloudLock, we would not be able to focus on policies. We’d be spending all of our time managing and transferring documents,” said Santacroce.

CloudLock lets domain administrators and document owners quickly and effectively verify the legitimacy of suspected exposures, remediate any incorrect sharing, and rely on ongoing monitoring to prevent any future exposures.

For more information on Teach For America, see: http://www.teachforamerica.org/
Collaboration Security Case Study

The IT team at Mattawan Consolidated School selects CloudLock for visibility, compliance monitoring and control for staff and students.

The Institution

Mattawan Consolidated School is a growing school district just west of Kalamazoo and Portage, Michigan. Covering approximately 52 square miles, this family-oriented, education-minded community is attracting residents from the surrounding area and is becoming home to individuals and families new to the Kalamazoo area.

Mattawan Consolidated School’s students receive a rigorous academic experience within outstanding facilities. The four schools that comprise the school district provide a core curriculum that exceeds the Michigan Department of Education’s requirements in all courses and integrates core state and national standards within the subject content.

The Challenge

With 400 staff and 4000+ students, the IT team at Mattawan Consolidated School is now tasked with maintaining the same level of controls for data stored in the cloud as it does with data stored on local file servers. Privacy and compliance continue to be the number one priority for the IT staff.

Enabling Google Apps for the school’s students allowed for effective collaboration without increasing IT expenditures. However, this also created a need to closely monitor students’ activities to make sure students continued to comply with the school’s code of conduct (i.e. ensure that no cyber bullying is happening).

“Take, for example, all the IEP documents (Individual Education Plan). The school owns hundreds of these documents, and each one contains sensitive and private information about each student participating in this program. It’s key that we have the visibility and control to make sure these documents comply with privacy regulations.”

— Pete Poggione, IT Director
Mattawan Consolidated Schools
The CloudLock Solution

After installing CloudLock for Google Apps on Mattawan’s staff domain, the IT team was able to find all sensitive documents, review and correct sharing permissions, and make sure they were complying with privacy regulations and best practices.

Poggione added, “With CloudLock for Google Apps, we regained the visibility and control of our documents and were able to audit all the documents and correct sharing permissions.

Compliance with Privacy Regulations

Using CloudLock for Google Apps allowed Mattawan Consolidated Schools to comply with privacy regulations such as FERPA and CIPA. With CloudLock they were able to:

• Find sensitive documents and adjust sharing permissions
• Notify data owners of exposed documents containing potentially sensitive data
• List documents that do not comply with sharing best practices
• Change or revoke excessive rights as a domain admin
• Audit permissions changes performed by all domain admins with an audit trail
• Schedule reports to run automatically

“CloudLock for Google Apps provides us the ongoing monitoring and control we need to make sure our sensitive documents comply with privacy regulations. With CloudLock we are also able to change permissions without going through the end-users every single time. This is a big time saver for us,” said Poggione.

Re-gaining Visibility and Control

“When using CloudLock for Google Apps we were able to see for the first time what sharing permissions we have on our documents and make sure we set the right controls in place” said Poggione.

CloudLock for Google Apps is a Google Marketplace application built on the Google Apps Engine that provides key IT data management insights like:

• Users inventory – who is using Google Docs and what documents they own
• Data Inventory – how many documents exist and which types?
• Which documents are shared with the ‘public’ or Internet?
• Which documents are shared outside the organization?
• Which documents are shared with ‘Everyone’ within the domain?
• Who has access to what and what is accessible to whom?

“We first needed visibility and then control. CloudLock for Google Apps gave us both. With CloudLock we were able to audit all the documents of a specific user, change ownership of these documents and adjust the sharing permissions to match our policies.”
"As many other Google Apps for Education users, we considered the buy vs. build options. We looked into developing scripts that would provide us some of this functionality and after evaluating CloudLock for Google Apps we have decided to stick to our core competency—education—and purchased a product that does what we need and more."

**Monitoring Student Activities**

Like most schools, Mattawan Consolidated School is subject to comply with The Children’s Internet Protection Act (CIPA). This means that they are required to adopt and enforce a policy to monitor the online activities of minors.

"In addition to the school’s staff, we have also enabled Google Apps for our students. With students, we face the challenge of making sure no bullying is going on. We are as committed to our code of conduct as much as we are committed to our academic excellence, and we needed the ability to prevent inappropriate use of our Google Docs for bullying," said Poggione.

CloudLock will soon release a feature that will enable admins to search a document’s content, allowing IT to search through student documents for inappropriate content without assuming ownership of these documents or changing the sharing permissions.

**Protecting Data In the Cloud**

For security conscious IT leaders leveraging Google Apps, CloudLock for Google Apps is the only cloud data protection solution that enables control of data while gaining the collaboration and cost savings benefits of Google Apps.

For more information on Mattawan Consolidated School, see: [http://www.mattawanschools.org/](http://www.mattawanschools.org/)
Collaboration Security Case Study

Edina Public Schools Selects CloudLock to Address Various eGRC (e-Discovery, Governance, Risk Management and Compliance) Needs.

At a Glance

Industry: K-12
Number of Staff and Faculty: 1170

Drivers for Google Collaboration:

- Collaborative capabilities among students and faculty
- Considerable cost savings in transitioning from on-site computing to the cloud

Requirements for Secure Collaboration

- Comply with HIPAA and CIPA regulations
- Ease of risk management by controlling the exposure of sensitive data

Consequences for Not Implementing Security Controls:

- Elevated risk of exposing sensitive information via public sharing
- Inability to easily manage the sharing properties of many documents at once

Primary CloudLock Collaboration Security for Google Apps Features Used:

- Security Policy Engine to detect violations of Acceptable Use Policies and enforce new policy guidelines
- Collaboration Security automated e-mail alerts for recently exposed documents
- Complete Audit Trail of all actions performed by administrators and end users

The Institution

Edina Public Schools is comprised of approximately 7,990 students, K-12, served by 1,170 teachers and support staff in six elementary schools (Grades K-5), two middle schools (Grades 6-9) and one senior high school (Grades 10-12). Edina Public Schools is committed to keeping class sizes as small as possible while retaining the educational support needed to ensure quality learning opportunities.

The reputation of Edina Public Schools continues to grow nationally in both academic excellence and technological innovation. The school was recently named one of ten global winners in Google’s “Gone Google Story” contest. Google recognized Edina’s innovative use of Google Apps to transform the way students and staff engage in learning and in global society.

The Challenge

Edina’s media and technology services team is a leading member of the Minnesota Technology Leadership Team and is recognized for its significant achievements in marshaling technology to transform learning for students. Contributing to these achievements was an initiative to go Google that took place early in 2010, using mail, documents and sites for its teachers and students.

With the enhanced collaboration came the need to support the organization from an operational perspective, manage data exposures, and comply with internal governance procedures and regulations.

“We realized that we needed additional tools to be able to respond quickly to eDiscovery requests, comply with regulations and effectively manage risky data exposures,” said Edina Public School’s Director of Media and Technology Services.

“CloudLock allows us to quickly respond to e-Discovery requests, giving us an effective way to comply with regulations like HIPAA and CIPA, and helps us manage risk by controlling the exposure of sensitive data.”

— Director of Media and Technology Services
Edina Public Schools
eGRC - for Google Docs and Sites

CloudLock enables organizations to fully enjoy the collaboration benefits and cost savings of the cloud while still performing all the management tasks and processes they need to fulfill different aspects of e-GRC.

The following CloudLock features help schools and other organizations meet their eGRC requirements.

**E-Discovery** – CloudLock supports the various steps of the e-Discovery process and makes it easy for organizations to produce the necessary documents required for litigation hold:

- Search to find all the relevant documents based on metadata and keywords. CloudLock’s advanced search capabilities give users the ability to search ALL the documents created or shared with your domain (including documents that you are not shared on explicitly).
- Copy and store relevant docs in a protected area where they cannot be deleted or modified by end users
- Extract the relevant documents for further processing

**Governance and Compliance** – CloudLock provides the visibility and control needed for compliance with Google Docs and Google Sites:

- Full visibility into all documents and sites in the domain
- Control permissions and access rights to enforce access controls by adding or removing collaborators, changing ownership, and changing collaborator access rights on all documents and sites in the domain
- Ongoing monitoring and alerting of the entire domain with email alerts on newly exposed documents and changes in permissions for existing documents
- Complete audit trail of all activities and changes performed. CloudLock provide a tamper-proof audit trail for changes and searches done via the application as well as a full audit trail for all user permission changes

**Risk Management** – CloudLock domain administrators gain access to a consolidated dashboard that provides an overview into users, documents, sites and exposure classification for the entire domain:

- Exposure classification of all the documents and sites in the domain
- View changes in ownership and changes for every document created or shared with your domain. Use ad-hoc reporting to see what has changed between any two dates
- Bulk operations to secure sensitive documents

"CloudLock allows us to perform data and exposure management. The various reports allow us to find and secure exposures and gives me an effective way to monitor usage, growth and collaboration patterns," said the Tech Specialist at Edina Public Schools.

For more information on Edina Public Schools, see: [http://www.edina.k12.mn.us/](http://www.edina.k12.mn.us/)

For more information on CloudLock Collaboration Security for Google Apps please contact sales@cloudlock.com.

To start a free trial of CloudLock for Google Apps visit [cloudlock.com](http://cloudlock.com).
The IT Team at Escondido Charter School District Selects CloudLock for Google Apps to Protect Sensitive Data Stored in the Cloud

The Institution

Escondido Charter School District (ECSD) is a back-to-basics school of choice serving students in San Diego County and adjacent counties. ECSD is a public school; there is no tuition. Accomplishment in academic areas is stressed with an emphasis on the understanding and appreciation of American Civilization and United States History.

Dennis “Coach” Snyder, a veteran educator and a thought leader in the charter schools community, started the school in 1996. The “Coach” also hosts Charter School Radio to share best practices, ideas and success stories of the growing charter school community. The radio show is best described as: “the voice for educational choice.”

The Challenge

Now, more than ever, charter schools are subject to strict budgetary constraints. The need to do more with less drove Escondido Charter School District to evaluate cloud solutions as a way to optimize and reduce IT expenditures.

Adopting Google Apps for Education for the school’s staff enabled the school to realize significant cost savings.

The school identified additional cost savings opportunities by using Google Docs as their cloud file server. To do that, the IT team at Escondido Charter School still needed to maintain the same level of data governance and protection to make sure that proprietary documents are shared correctly and no sensitive data is exposed.

“Using Google as a collaborative platform and storing documents in the cloud turned out to be a major cost savings initiative. With CloudLock, we were able to further cut our capital expenses by moving all our documents to the cloud.”

— Jared Planter, IT Manager
Escondido Charter School District
The CloudLock Solution

Enabling CloudLock for Google Apps in Escondido Charter School District's staff domain allowed the IT team to realize the full benefits of using Google Docs as their cloud file server.

With CloudLock for Google Apps, the IT team was able to:

- Gain visibility for all document sharing settings
- Fix document access rights
- Audit all documents and all users - see who has access to what, and what is accessible to whom
- Change ownership of documents to prevent data loss when terminating accounts or accommodating role changes

Realizing the Cost Savings Benefits of Google Apps

CloudLock for Google Apps provides visibility and control of documents stored in the cloud, enabling companies to fully benefit from the online file server by moving even the most sensitive documents to the cloud.

“CloudLock for Google Apps enabled us to move all our documents to the cloud, including sensitive documents that we previously kept on-premise. Every file server that we no longer need to purchase adds directly to the bottom line and allows us to focus on our core business – delivering the highest quality education,” said Planter.

Enabling Google Docs for Students

“Like many other educational institutions, our staff and students are on different domains. CloudLock made it possible for us to enable Google Docs for the school’s students as well,” said Planter.

Students are now benefiting from the online collaborative suite while the IT team is able to keep an eye on their activities to comply with ‘The Children’s Internet Protection Act’ (CIPA).

Escondido Charter School is committed to provide a safe and orderly learning environment, with a strict no bullying policy enforced among the school’s students. CloudLock makes it possible for students to benefit from Google’s collaborative suite while maintaining regulatory compliance and codes of conduct.

For more information on Escondido Charter School District, see: http://escondidocharter.org/