GAT Labs
for education

End-of-Year Google Workspace for Education Audit

School Admin Guide

TABLE OF CONTENTS

In the age of technology-driven classrooms, secure and efficient management is a complex task. That's why auditing the Google Workspace environment regularly is essential. It helps admins to spot and address security risks, enhance student online safety, and report on compliance.

This guide walks you through a recommended year-end Google Workspace audit. It provides practical steps to review essential aspects of your domain using the GAT Labs tools: **GAT+, GAT Shield, GAT Flow,** and **GAT Unlock.**

Why is an Annual Google Workspace Audit Important?

Reviewing the Google Workspace environment during the summer break helps institutions remain a safe, productive, and trustworthy learning space for the upcoming school year.

- **Gain Compliance Audit Readiness:** Automatically report across your domain on compliance with key data privacy requirements.
- **Eliminate Security Gaps:** Detect potential cybersecurity risks by auditing user permissions, file shares, inactive user accounts, and app privileges.
- **Strengthen Student Safety:** Evaluate and improve the school's online safety policies, and schedule reports on user online activity.

1. User Offboarding & Audit

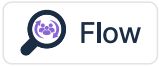
At the end of every school year, large numbers of students and many teachers leave educational institutions. Without automated offboarding, this process requires significant time, effort, and attention from IT teams. They need to deactivate leavers' accounts while maintaining operational continuity and protecting the school's data.

Besides the offboarding process, the end-of-year season is the perfect time to audit any hidden, inactive, or suspended user accounts your domain may still hold that consume excessive Drive storage space and user licenses.

The Risk

During manual offboarding of multiple users, it's easy to overlook or unnecessarily remove user file shares, access permissions, or classroom owners. Additionally, large files owned by inactive users may still take up Drive storage space.

Admin's Actions:

1. Customized Offboarding Workflow 

Create a set of actions to be done when offboarding a student or a teacher. It will run automatically when you start the workflow. You can customize each workflow to your school's needs.

Student Offboarding Workflow Actions (examples):

- Force sign out
- Change user password
- Remove the user from classrooms, all groups, and chats
- Remove user access to the school's files and folders
- Delete user calendar events and unshare the user calendar
- Change ChromeOS device status (to deprovision a school device used by the student)
- Remove email forwarding
- Suspend user
- Archive user (to reduce Google license costs)
- Delete user (after a retention period)

Teacher Offboarding Workflow Actions (examples):

- Force sign out
- Change user password
- Change the classroom owner (to keep instructional continuity)
- Remove the teacher from classrooms
- Migrate the user's Drive and Google Keep (to maintain access to their learning resources)
- Google application data transfer
- Set up an auto reply
- Remove email delegation and email forwarding
- Transfer calendar events and remove the user from all calendars
- Change ChromeOS device status (to deprovision a school device used by the teacher)
- Suspend user
- Archive user (to reduce Google license costs)
- Delete user (after a retention period)

2. Inactive Accounts Clean-up  

Even if you audit and automatically offboard users each year, inactive accounts may still remain in your Google Workspace, draining storage space and generating extra costs.

Clean up unused Google accounts:

- Identify inactive and repetitive accounts by the last login date.
- Transfer their Drive file ownership.
- Delete inactive accounts to decrease the number of licenses.

Free up Google Drive storage space:

- Identify large and inactive files and folders in all Drives.
- Identify users who use the most space on Google Drive.
- Save files you need externally, transfer large files from users to yourself, and remove them from the original Drive.

Learn from the GAT Labs Blog:
How to automate offboarding in Google Workspace?

2. Access Control Audit

Both active and inactive user accounts can inadvertently create security gaps that allow unauthorized access. That gateway can be a sensitive file shared publicly or a third-party app to which the user granted too broad privileges. Regular access control audits help prevent data breaches and accidental exposure.

The Risk

Unmonitored external apps' privileges, file sharing, and overly high user access levels are top security risks in Google Workspace for Education. They pose a serious threat to sensitive data stored in your school's domain.

Admin's Actions:

1. File Shares Review GAT+

Audit **files shared externally** and consider whether these permissions are still necessary. You can notify users about these file shares using the Scheduled Reports feature or remove them immediately.

Audit all **external files shared in your domain** to detect externally owned files and remove your domain's access to them if needed.

GAT+ is the only tool on the market that reports files shared with your domain from outside your environment (files shared in from external users).

2. User Access Permissions Audit GAT+

Review current permissions for specific users and groups. If needed, change user permissions and file ownerships to meet your school's needs. Consider automating this bulk modification with a custom workflow that runs when an event occurs, for instance, when a user is suspended.

3. Third-party Privileges Assessment GAT+

Go to the section "Third-Party & Browser App Governance." (page 9).

Learn from the GAT Labs Blog:
How to implement secure user access permissions management?

3. Compliance & Online Safety Policies Audit

Staying compliant becomes challenging in the digitalized world of education. It's an ongoing responsibility that lays the foundation for student online safety and data security. While it's a routine task, reviewing online safety status at the end of the year will help you reinforce your school's compliance and policies.

The Risk

For educational institutions, non-compliance with key data privacy regulations (CIPA, COPPA, FERPA, GDPR, ISO 27001) threatens student online safety and can result in the loss of public funds and fines.

Admin's Actions:

1. Student Online Safety Policies Check Shield

Review your current web filtering settings for students. Make sure the safe-browsing policy covers all age-inappropriate, harmful, and potentially disturbing content, both as specific websites and keywords.

Audit triggered alert rules and the entire online browsing activity across the last year. Identify emerging online threats, such as visiting unknown websites, using new AI apps, or wellbeing-related searches done by your students. Update your policies accordingly.

Schedule reports regularly for continuous monitoring.

2. CIPA Compliant Category Shield

Enable the pre-configured web filtering category that blocks online content to comply with CIPA requirements. It covers:

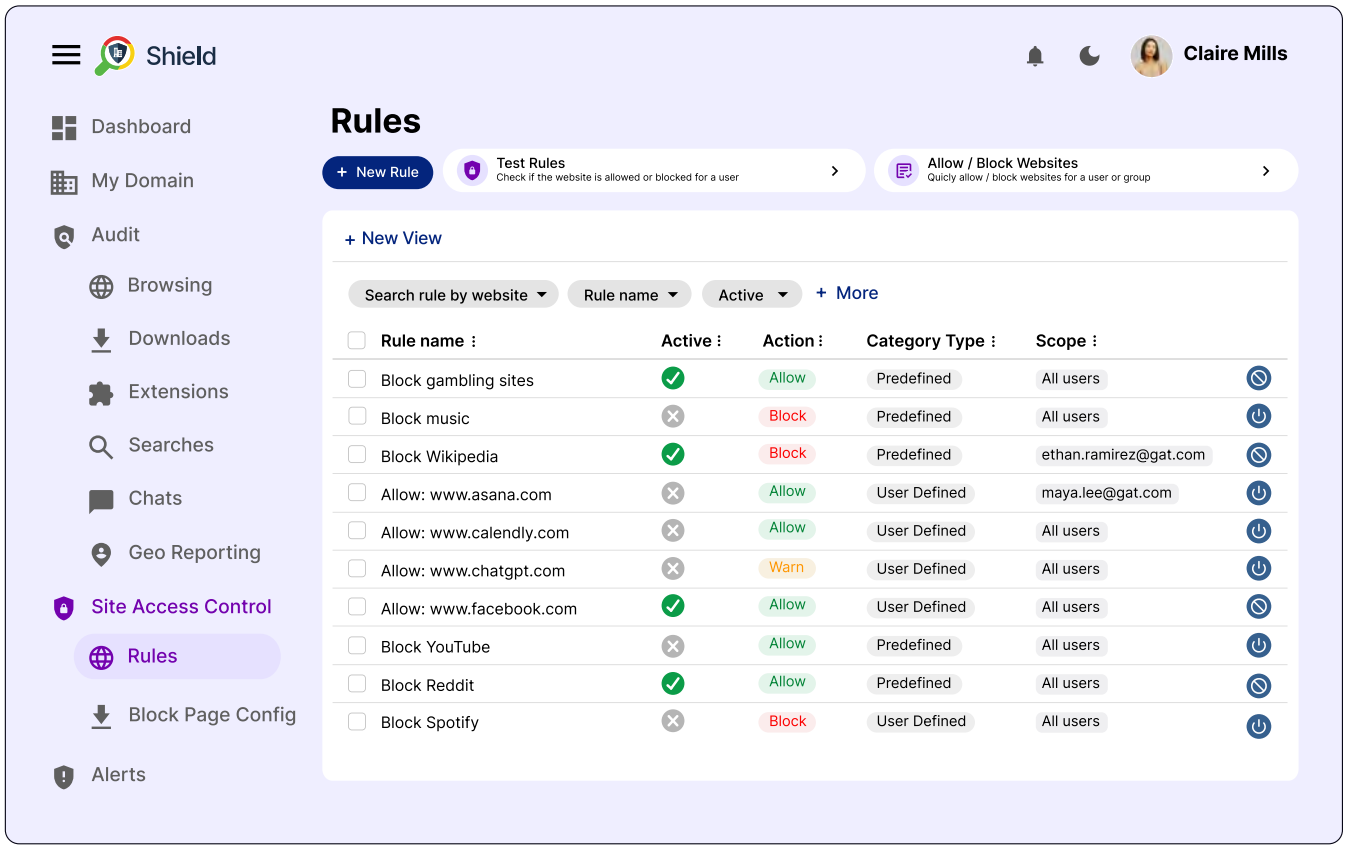
- Over 8 million inappropriate sites
- Customizable keyword-based filters
- YouTube access restrictions
- Strict Safe Search for both words and images on Google

3. Sensitive Data Protection Policy GAT+

For files and folders containing sensitive information, set up a customized DLP policy to protect data from unauthorized access and monitor user activity on these files. The policy can include, among others:

- Removing all shares
- Removing all external shares or removing all except xyz
- Replacing “Public” with “Public at your domain” or “Public with link.”

Learn from the GAT Labs Blog:
How to ensure compliance in Google Workspace?



4. Third-Party & Browser App Governance

Increasingly popular AI-powered tools and third-party apps boost productivity in the classroom, but their usage is harder than ever to manage and oversee.

When uncontrolled, they create security blind spots, potentially exposing personal data and leaving no audit trail in the event of a data breach.

Frequent users' practice of logging in to an app with a Google account poses an additional challenge, as it may grant the software access to the user's Gmail, Shared Drive, and other internal data.

The Risk

Unmonitored third-party apps and browser-based tools may risk sensitive data privacy and the school's compliance.

Admin's Actions:

1. Third-Party App Risk Assessment GAT+

Review all applications currently installed in your Google domain. The audit will show you for each app:

- What users installed it
- Requested privileges
- Scope risk score

2. Third-Party Apps Policies Update GAT+

If an app was flagged with a "moderate" or "high" risk score in the assessment, consider restricting or banning it.

Add the app to the banning policy for the entire school or just a specific OU. GAT+ will revoke all access users have granted to the app and ban it in real time whenever a user attempts to install it and grant it privileges again.

3. AI Browser-Based Tools Audit Shield

Access users' online activity history for the last year. Identify AI-related websites and evaluate whether they are safe or should be restricted.

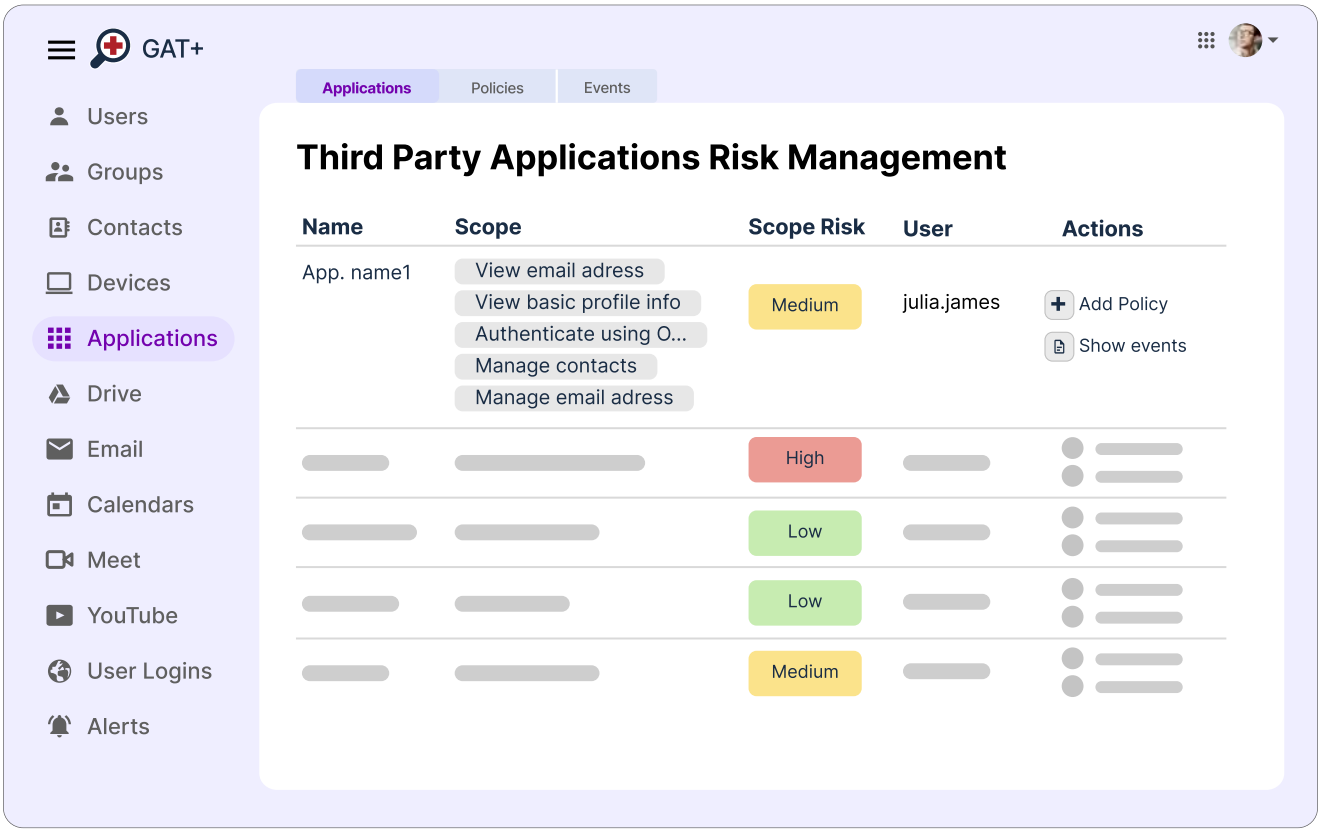
For potentially harmful or suspicious websites, set up an alert rule that will notify you next time a student tries to access them.

4. Google Gemini Audit [Google Admin Console]

Review Gemini's usage in Google Workspace apps per OUs and each user:

- The number of active Gemini users
- Gemini daily usage
- Users who have reached AI feature limits

Learn from the GAT Labs Blog:
How to handle Shadow AI in schools?



5. Security Review & Real-time Monitoring

Security is a complex area interconnected with all aspects of domain auditing mentioned above, and much more. In the technology-driven world, ensuring a secure learning environment requires more admin efforts than ever. Only a structured management strategy and real-time monitoring allow IT teams to detect threats early, protect data, and comply with school policies.

The Risk

The lack of real-time cybersecurity controls makes schools vulnerable to common threats to educational institutions: phishing, ransomware attacks, and data breaches.

Admin's Actions:

1. Annual Security Report GAT+

Generate an overview of the key metrics (file sharing, access permissions, and user online activity) for the last school year. Audit for cybersecurity incidents if they occurred, and update your policies to prevent them in the future.

2. Automated Security Reports GAT+

Schedule automated reports to track the domain's security status, detect emerging threats early, and be ready for a compliance audit.

3. Real-time Security Monitoring Shield

Audit user browsing activity in the Chrome browser for the selected timeframe. Create scheduled reports for a specific group of users (e.g., students), which show:

- Full browsing activity
- User downloads
- Used extensions and their events
- Chats activity
- User & device geo reporting

Learn from the GAT Labs Blog:
How to protect school data from phishing attacks?

Useful Resources

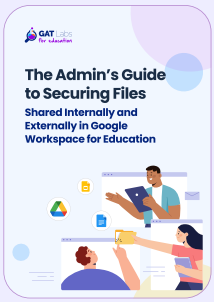
Equip your institution with the knowledge and tools needed to defend against digital threats effectively.

Dive deeper into security and management for Google Workspace for Education with our guides for school admins:

Read more

In this comprehensive guide, we'll walk you through the essential steps to effectively audit your Google Workspace for Education.

Read more



Learn how to review and manage AI app access in Google Workspace to ensure data security and a safe AI experience for your school.

Read more

Discover unique GAT Labs features for effective file share auditing and management in Google Workspace for Education.

Read more

GAT Labs for education

If you have any questions or need assistance with your end-of-year auditing, our Support Team is always ready to help you.

If you've seen GAT Labs features in this guide that aren't available within your current plan, book a demo to see how we can enhance your Google Workspace.

Visit our Website

Training Sessions Calendar

Schedule a Live Demo