GAT Labs for education

The Admin's Guide to Securing Files

Shared Internally and Externally in Google Workspace for Education

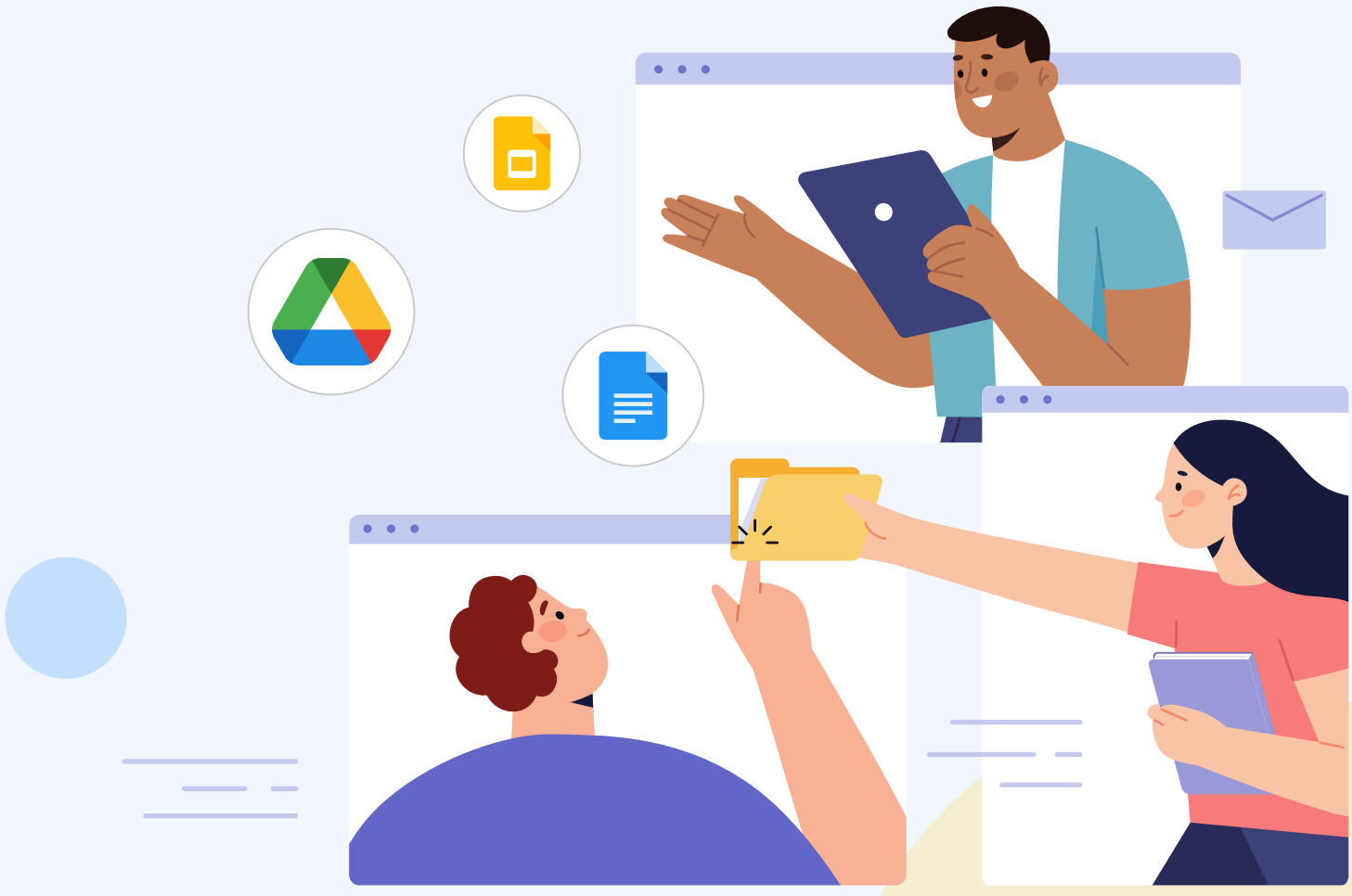


Table of Contents

Google Drive streamlines classroom management, school administration, and collaboration between students and teachers, but uncontrolled file sharing within and outside the school can pose security and safety risks.

This guide provides **actionable steps for monitoring files shared internally and files shared externally**, ensuring robust data security and compliance across your Google Workspace for Education.

1. Understanding Google Drive Sharing Permissions

A well-organized permission structure is essential for managing data access. Drive permissions include Viewer, Commenter, and Editor levels, each allowing different degrees of access to information.

It's crucial to:

- Review and assign permissions based on user roles, avoiding unnecessary Editor permissions.
- Set default internal and external sharing settings in the Google Admin Console, restricting access to sensitive files.

Steps:

1. Go to *Admin Console* > *Apps* > *Google Workspace* > *Drive and Docs* > *Sharing Settings*.
2. Configure internal and external sharing defaults to limit unnecessary exposure.

2. Auditing Files Shared Externally

Regular audits of files shared externally can prevent unauthorized access. Use Google's File Sharing Exposure report to gain insight into shared files and ensure only authorized users retain access.

How to Conduct an Audit

- Open the Admin Console and navigate to *Reporting* > *Drive Audit*.
- Review shared files and their access levels, particularly for external shares.

Automate Audits with GAT+: Including Share-in Files

Reporting:

- Create automated reports of files shared externally, allowing you to detect any sharing anomalies quickly.
- Learn how to generate automated reports with GAT+ here.

Identify External Ownership:

- GAT+ highlights externally owned files (marked in orange under the "Owner" heading), making them easy to track.
- Use this guide to find and act on externally shared files.

Advanced Search Operators:

- Leverage unique search operators in GAT+ to track when files were initially shared into your domain.
- Learn about file-sharing policy violations and alerts here.

Actionable Insights:

- Automatically remove external shares according to the time-based policies (details).
- Replace "Public" or "Public with Link" sharing with more secure settings (guide)

Drive Audit Filters:

- Use search filters to pinpoint sensitive information or specific file types (details).
- Apply a search filter for files based on metadata or ownership (guide).

File Permission Restoration:

- Restore permissions on files removed by policies (details).

Next Steps for Admins

1. **Monitoring and Alerts**
   - Set alerts for file-sharing violations and unusual activity (guide).
   - Monitor Drive file activity with alert rules (details).
2. **Action on External Files**
   - Automate actions such as removing permissions for files shared externally (guide).
3. **Shared Drive Management**
   - Export and analyze shared Drive data for comprehensive reporting (details).

Key Capabilities

Scheduling Reports:
Set daily, weekly, or monthly reports for recently shared in files, ensuring a regular audit of external shares.

Unique Search Operators:
GAT+'s search operator tracks when files were initially shared internally, an advanced feature not available through Google's API.

Pro Tip:
Use GAT+'s alerts for files newly shared internally to ensure admins have visibility over shared data in real time. For more details, view our Knowledge Base article.

3. Structuring Files Shared in Google Drive

Organizing files shared in Google Drive is crucial for data access control. A well-thought-out Shared Drive layout helps admins manage permissions and segment data access effectively.

Best Practices for Structure

- Organize by classroom, grade, faculty, or role to restrict access based on specific needs.
- Set permissions at the folder level within Shared Drives, allowing each sub-folder to have more refined controls.

Using GAT Shield for Enhanced Control

- GAT Shield allows admins to monitor permission changes and ensure the structure remains secure.
- It offers real-time alerts for any modifications in file access, helping maintain control and compliance in Google Drive.

Practical Example

- For each grade, create an "[Number] Grade" Shared Drive with subfolders like "Students," "Subjects," and "Assignments." Assign permissions so only relevant students and teachers have access to specific subfolders.

Best Practice:
Regular audits minimize risks, especially for sensitive files. Schedule monthly reviews to stay proactive.

4. Managing and Tracking External File Shares

Tracking external shares is essential to prevent sensitive data from leaving the educational institution.

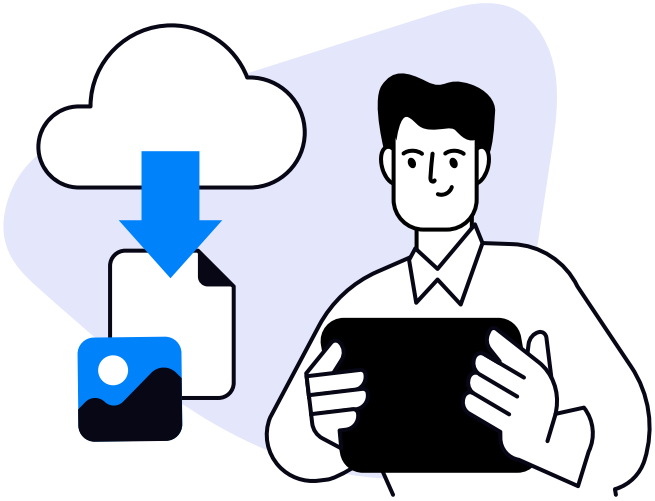
How to Find Files Shared Externally

- Use GAT+ to locate all files shared externally in Google Drive. This can include any documents, pictures, or presentations shared outside the school.

Steps to Manage External Sharing

- In GAT+, use filters to display only externally shared files.
- Review permissions, especially for files shared publicly, and adjust as necessary.

> **Risk Mitigation Tip:**
> Restrict external sharing for sensitive documents like student personal databases.



5. Proactive Data Loss Prevention for Shared Files

Data Loss Prevention (DLP) policies help Google Admins protect sensitive information proactively. Configure DLP rules for files shared externally to monitor activity that could lead to data leaks, such as unauthorized downloads or sharing.

Setting Up DLP Alerts

- In the *Google Admin Console > Security > DLP*.
- Create rules that trigger alerts if sensitive data is shared externally, such as personal data, banking information, or health reports.
- Use GAT+ to extend DLP to real-time monitoring for high-risk files.

Practical Steps for Protection

- Set up alerts for printing, downloading, or copying sensitive data.
- Use content detectors to flag specific keywords like "confidential" or "sensitive" in documents shared externally.

6. Handling Files Shared In From External Parties

Managing files shared from external sources in your school is essential to maintain data security. While the Google Admin Console provides basic visibility, GAT+ significantly enhances your ability to monitor and act on these incoming shares.

Using the Google Admin Console

Admins can review shared-in files by navigating to *Reports > Drive Audit Log* in the Admin Console:

1. Filter by events such as Incoming File Shares or External Sharing.
2. Identify files shared from outside domains to ensure compliance.

For further guidance on Drive audits in the Admin Console, refer to Google's support documentation.

Enhanced Management with GAT+

1. **Comprehensive File Tracking**
   - GAT+ allows you to see real-time insights into files shared in from external domains.
   - Use the Drive audit to identify external files marked with a unique color (orange) for quick identification (guide).
2. **Set Up Alerts**
   - Create alert rules for incoming files from specific domains or users to prevent unauthorized sharing (details).

3. **Scheduled Reports**
    - Automate reports for recently shared-in files with details like file type, owner, and sharing status (guide).
    - Regular audits ensure that only trusted sources can share sensitive data with your school.
4. **Policy Enforcement**
    - Automate the removal of external shares that do not comply with organizational policies (details).
5. **Advanced Search Options**
    - Use GAT+'s unique search operators to locate files based on specific criteria, such as sharing source or timestamp (details).

Next Steps for Admins:

1. **Set Up Monitoring:**
    - Use Drive alerts to track sharing behavior in real time (guide).
2. **Regular Audits:**
    - Schedule reports for external files and review anomalies to ensure compliance.
3. **Policy Management:**
    - Automate workflows to secure sensitive data and enforce organizational policies (details).

7. FAQs on File Sharing in Google Drive

Q: How often should I audit files shared externally?
A: Monthly audits are ideal for high-security environments. Use GAT+ to automate this process and receive alerts on new external shares.

Q: How can I prevent sensitive files from being shared externally?
A: Configure DLP policies and enforce permissions in the Admin Console to control external sharing.

Q: How can GAT Labs tools help with managing shared files?
A: GAT+ and GAT Shield offer advanced tools to enhance visibility, set up real-time alerts, and generate detailed reports for files shared both internally and externally. These features simplify Google Drive management, ensuring robust security and compliance with your organization's data policies.

Q: How can I restrict file-sharing settings for specific classrooms or teams?
A: In the Admin Console, customize sharing settings by organizational unit (OU). This allows you to limit external sharing permissions or disable sharing for sensitive teams, such as finance or HR, enhancing data security. GAT+ can help track and enforce these settings.

Q: What's the best way to handle file ownership transfers when offboarding teachers?
A: Use GAT Unlock to securely transfer ownership of departing teachers' files. This ensures no critical files are lost and prevents ex-employees from accessing shared data.

GAT Labs
for education

Strengthen Your Google Drive Security & Protect Student Data With GAT Labs

Schedule a Demo

15-Day Free Trial