

# Preventing and Investigating Abuse and Inappropriate Content Checklist

Google Workspace for Education paid editions ([Education Standard](#), [Teaching and Learning Upgrade](#), and [Education Plus](#)) help you create an innovative learning environment with enterprise-grade tools that are customized for education. Here we'll provide guidance on actions you can take to help prevent and investigate abuse and inappropriate content.

## Exploring Google Workspace for Education for the first time?

Connect with an expert and learn more [here](#).

We recommend that Google Workspace administrators take some basic steps to help prevent abuse, including:

- Enable Data Loss Prevention (DLP) for [Gmail](#) and [Drive](#). DLP gives you control over what content users can share, and prevents unintended exposure of sensitive information such as credit card numbers or identity numbers.
- Review [these best practices](#) to improve the security of your administrator accounts, and follow [this security checklist](#) when applying settings across your Workspace apps. You can also use [Security Health](#) to monitor the configuration of your security settings and get recommendations based on best practices.
- Set [admin privileges to protect user privacy](#)
- [Maintain data security](#) after a user leaves your institution
- [Set up rules](#) to be notified of specific activity within your domain
- Implement [login protections](#) to help prevent unauthorized access or attacks on user accounts
- If you use a third-party CASB, [follow these guidelines](#) for integrating with Google Workspace