Overview and Benefits

Implementing these ChromeOS™ and Google Admin™ security settings helps the district create a safer, more consistent, and academically focused digital environment. Collectively, these controls reduce exposure to unapproved apps, prevent attempts to bypass filtering or disrupt instructional tools, and maintain the integrity of digital assessments. Students benefit from a distraction-free and equitable learning environment that protects their data and supports responsible device use. Educators benefit from fewer technology disruptions, more time for instruction, and a reliable digital ecosystem aligned with district goals.

Note: Google Admin console menus and settings are updated regularly, so menu names or navigation paths may change over time even though the underlying settings remain the same.

For additional learning resources, please visit us on the web here.
Need an account? Register here for our online training video series.

Disabling Access to Install Extensions

What this function does:

This setting prevents users from freely installing Chrome™ extensions or apps from the Chrome Web Store™ or Google Play Store™. Instead, all extensions must be approved and allow listed by administrators. This ensures only vetted, safe, and instructionally relevant tools can be added to student devices.

• Open the Google Admin console (admin.google.com).

• Navigate to Devices > Chrome > Apps & extensions > Users & browsers.

• Select the appropriate Organizational Unit (OU).

• Open Additional Settings.

• Edit Allow/block mode and set Google Play Store and Chrome Web Store to Block all apps, admin manages allowlist.

• Click Save.

Disabling Developer Tools

What this function does:

This setting blocks the Chrome DevTools panel, which allows users to inspect page code, manipulate scripts, bypass filtering, or interfere with web applications.

• Open the Google Admin console.

• Go to Devices > Chrome > Settings > Users & browsers.

• Select the appropriate OU.

• Search for “Developer Tools” in User Experience.

• Set Developer Tools to Never allow use of built-in developer tools.

• Click Save.

For additional learning resources, please visit us on the web here.
Need an account? Register here for our online training video series.

Disabling Bookmarklets

What this function does:

By blocking URL patterns like javascript://* and data://*, this setting disables bookmarklets—small bits of JavaScript® saved as bookmarks. These are often used by students to bypass content filters or alter web pages.

- Go to Devices > Chrome > Settings > Users & browsers.
- Search for "Blocked URLs".
- Add javascript://* and data://* to the Blocked URLs list.
- Click Save.

Disabling Chrome Search Suggestions

What this function does:

This setting disables search and URL suggestions in the Chrome address bar (omnibox). By preventing predictive search suggestions and autofill prompts, districts can reduce distractions, limit exposure to inappropriate or unvetted content, and help ensure students remain focused on instructional tasks and approved resources.

- Open the Google Admin console.
- Navigate to Devices > Chrome > Settings > Users & browsers.
- Select the appropriate OU.
- Search for Search suggestions or Omnibox.
- Disable Search suggestions and URL prediction.
- Click Save.

Disabling Google Lens (Updated for 2026)

What this function does:

This setting disables Google Lens™ features such as the Lens overlay, the New Tab Lens button, camera-assisted search, region search, and the Lens website (lens.google.com). These features allow students to photograph questions or highlight content and instantly retrieve answers online.

- Go to Devices > Chrome > Settings.
- Select the appropriate OU.
- Search for "Lens" in Users & browsers.
- Disable Google Lens Overlay.
- Disable New Tab Page Google Lens button.
- Disable Camera-Assisted Search and Region Search.
- Navigate to URL Blocking and add https://lens.google.com.
- Click Save.

LockDown/Secure Browser Option

Curriculum Associates' LockDown/Secure Browser option helps maintain the integrity of digital assessments by creating a focused, controlled testing environment. It restricts access to unapproved tools and features—such as browser extensions, developer tools, and Google Lens—that could introduce distractions or compromise test security.

For more information or to determine whether this option is right for your district, please contact your **partner success manager**.