



Chromebook and Google Workspace for Education Management

Google for Education



Chromebook and Google for Education Management

This document is a Chromebook and Google for Education Quick Start Guide for schools and describes (in greater detail):

- The benefits of managing Chromebooks with the [Chrome Education Upgrade](#)
- [Setup and enrolment](#) to efficiently enroll devices in your domain.
- [Device settings](#) to ensure your devices are set up to create an optimal learning environment.
- [User settings](#) to ensure that policies are in place to create an optimal learning environment.
- Information around how to utilise [Android Apps](#) on your domain.
- Information about viewing and managing your fleet of [devices](#).
- [Wi-Fi settings](#) to ensure your Chromebooks connect automatically to your network.
- [Google Vault](#) settings to support your organisation's retention and eDiscovery needs.
- [Google Workspace for Education Plus](#)
- [Support and Troubleshooting](#) options.

Chrome Management Overview



Terminology & Key Concepts

Policy

Setting that are defined in the Admin Console
Apply to Users or Devices

Admin Console

<https://admin.google.com>

Single place to manage Users and Devices

Note: *you will need to have been granted access to the admin console*

Organizational Unit (OU)

Container for Users, Devices, Settings etc.

Sub OU

- Inherits from parent OU
- Can overwrite inherited settings

Google for Education

Shareable devices and collaborative tools built for teachers and students



Google Workspace
for Education



Device Settings vs User Settings



Device Settings

Applies to the device with or without logged in user

- Controls who can login and how they authenticate
- View device details within the Admin Console
- Controls updates, auto-enrollment and device deactivation

Controls how the device operates, rather than what a user can do on the device



User Settings

Applies to the logged in user on any device

- Device does not need to be enrolled on the user's domain
- Manages the Apps, Extensions, Bookmarks etc that the user sees once logged in
- Manages the security profile for the user

Controls the user experience, not the device

Note: [Chrome Education Upgrade](#) is required to apply device settings

Chrome Education Upgrade

To manage Chrome devices across your organisation, you need a Chrome Education Upgrade for each device you want to manage.

This allows you to view and manage your enrolled device fleet from the Admin console.



1-time upgrade that lasts the life of the device



What if devices aren't managed with the Chrome Education Upgrade?

- Students can use Guest Mode or sign in with any account - in which case, no user settings will be applied.
- Lost/stolen devices can be used by anyone.
- Large amounts of time and effort are required to manage devices on an individual basis.

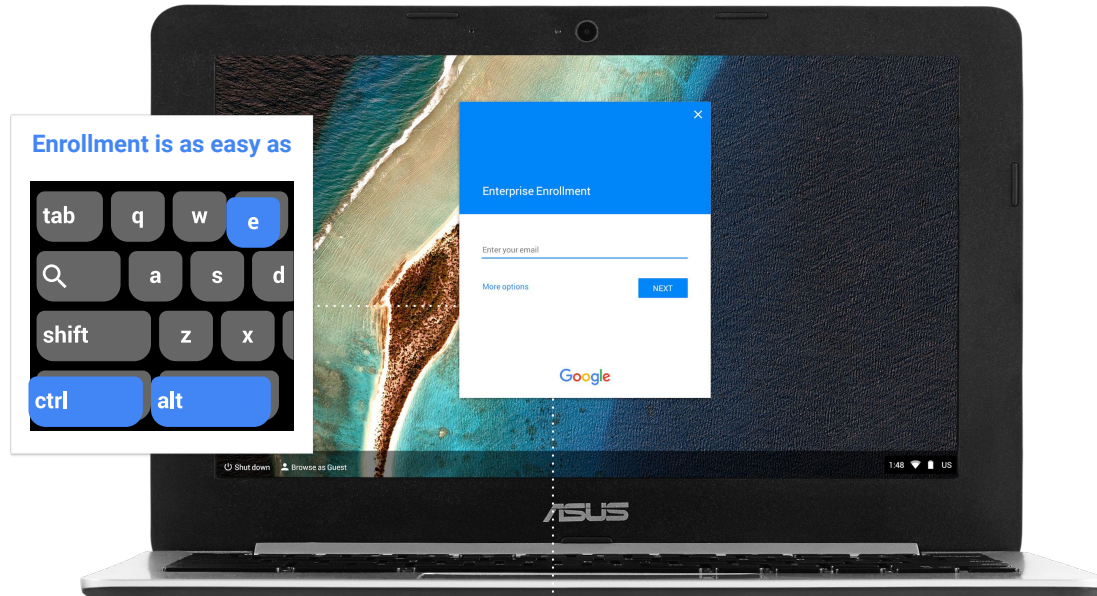


Device Enrollment



Note: General information within this section has come from [Google's Device Enrolment Support Website](#). Any recommendations are what The Warehouse Group Business consider best practice for NZ schools.

Just sign in once to lock the device to your domain

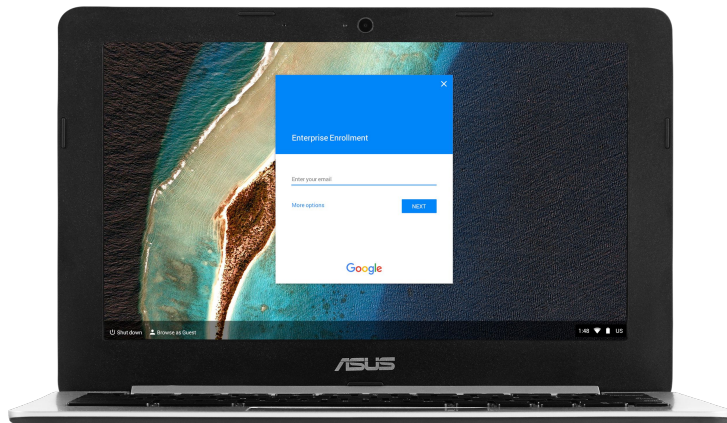


Before you start:

By default, devices automatically enroll into the top-level organisation. If you want devices to automatically enroll onto a specific OU (i.e 'Chromebooks') as well as being able to enter identifying information about the device, see [Give Chromebooks an Asset ID during enrollment.](#)

Device Enrollment

- 1 Click “**Let’s go**”, then Enter wifi details
- 2 Accepts T’s and C’s - Device updates at this point
- 3 Enroll the Chromebook (**Ctrl + Alt + E**) before signing in.
- 4 Username: **xxxxxxx** Password: **xxxxxxx**
- 5 Asset ID
Device name: **xxxxxxx** Location: **xxxxxxx**



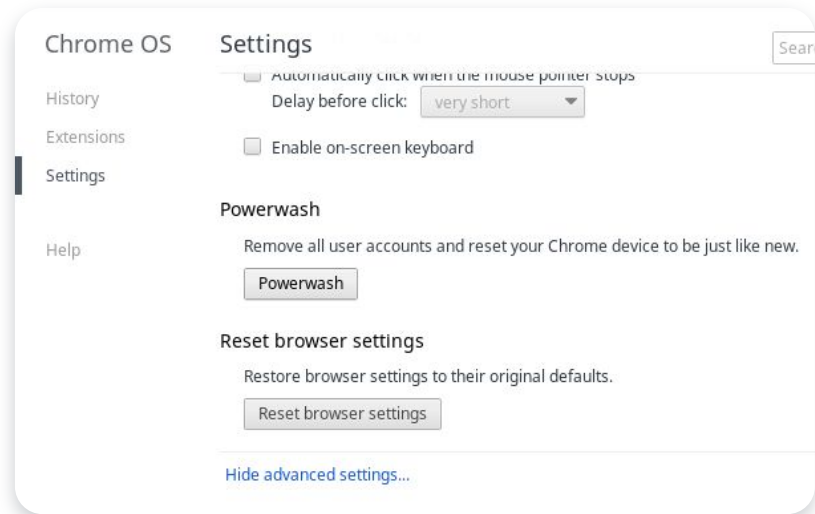
To give devices an Asset ID at this stage, be sure to enable this in your Admin Console first - see [Give Chromebooks an Asset ID during enrolment.](#)

What if my device has been logged into already?

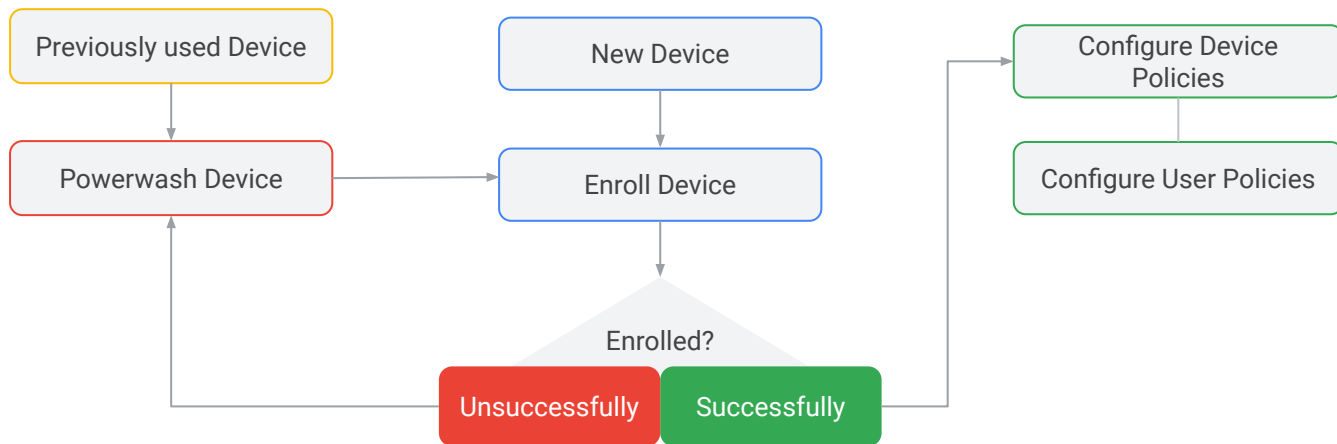
Device Reset: Powerwash

- Perform Factory Reset - Powerwash
- Removes all locally stored data & Google Accounts
- Shortcut: **Ctrl+Alt+Shift+R** at Sign-In screen

Once the device has been reset, you can then perform the steps to [enrol the device](#).



Device State Enrollment Process



*Note a previously enrolled device may be locked to a specific domain and prevent enrollment into another domain. Ensure that it has been [deprovisioned](#) and [wiped](#).

Devices - Give them an Asset ID

- Individual Chromebooks will need labelling in some way so that they can be identified easily.
- When the Chromebook label matches the Asset ID in the admin Console, it will be easier to:
 - find devices in the Admin Console
 - disable, deprovision, move to different OU's etc
- Asset ID's can be as simple as A1, A2, A3 for school-owned devices or the students name for BYO-devices.

<input type="checkbox"/>	Serial Number	Status	Asset ID	Enrollment Date
<input type="checkbox"/>	5CD433128T	Provisioned	Chromebook 1	May 18, 2016 8:51:57 AM

Give Chromebooks an Asset ID during enrolment

- Before enrolling your Chromebooks, consider creating an [Organisational Unit \(OU\) called 'Chromebooks'](#).
- For enrollment purposes, create a user such as `cb@domain.school.nz`
- Make sure this user is placed within the OU 'Chromebooks'.
- Go to User settings, select the OU 'Chromebooks' and ensure that the settings on the following page are in place.

<input type="checkbox"/>	Serial Number	Status	Asset ID	Enrollment Date
<input type="checkbox"/>	5CD433128T	Provisioned	Chromebook 1	May 18, 2016 8:51:57 AM

Note: for BYOD, consider creating [sub OU's](#) depending on whether you want some devices to utilize the [off-hours settings](#). Create a unique user within that specific organisation for enrollment purposes (i.e [ofo@domain.school.nz](#) to place devices in the Off Hours On OU)

Asset ID on enrolment & place devices in a chosen OU

Device management > Chrome > User Settings

ORGANIZATIONS

Search settings

Chromebooks

Enrollment Controls ⓘ

Device Enrollment

Inherited

Place Chrome device in user organization during manual enrollment. ⓘ

Place Chrome device in user organization ▼

Asset Identifier During Enrollment

Inherited

Populate Asset ID and Location fields during enrollment. ⓘ

Users in this organization can provide asset ID a ▼

Enrollment Permission

Inherited

Enrollment Permission ⓘ

Allow users in this organization to enroll new or i ▼

This settings ensures that when a device that is enrolled using the cb@domain.school.nz, you will be prompted to add an Asset ID and location for that device. Note: the location is where the device is likely to be (i.e Library), not the OU. This can be left blank if that suits.

These settings ensures that any device that is enrolled using the cb@domain.school.nz will automatically be placed the the 'Chromebook' OU.

Device Settings



Note: General information within this section has come from [Google's Device Settings Support Website](#). Any recommendations are what The Warehouse Group Business consider best practice for NZ schools.

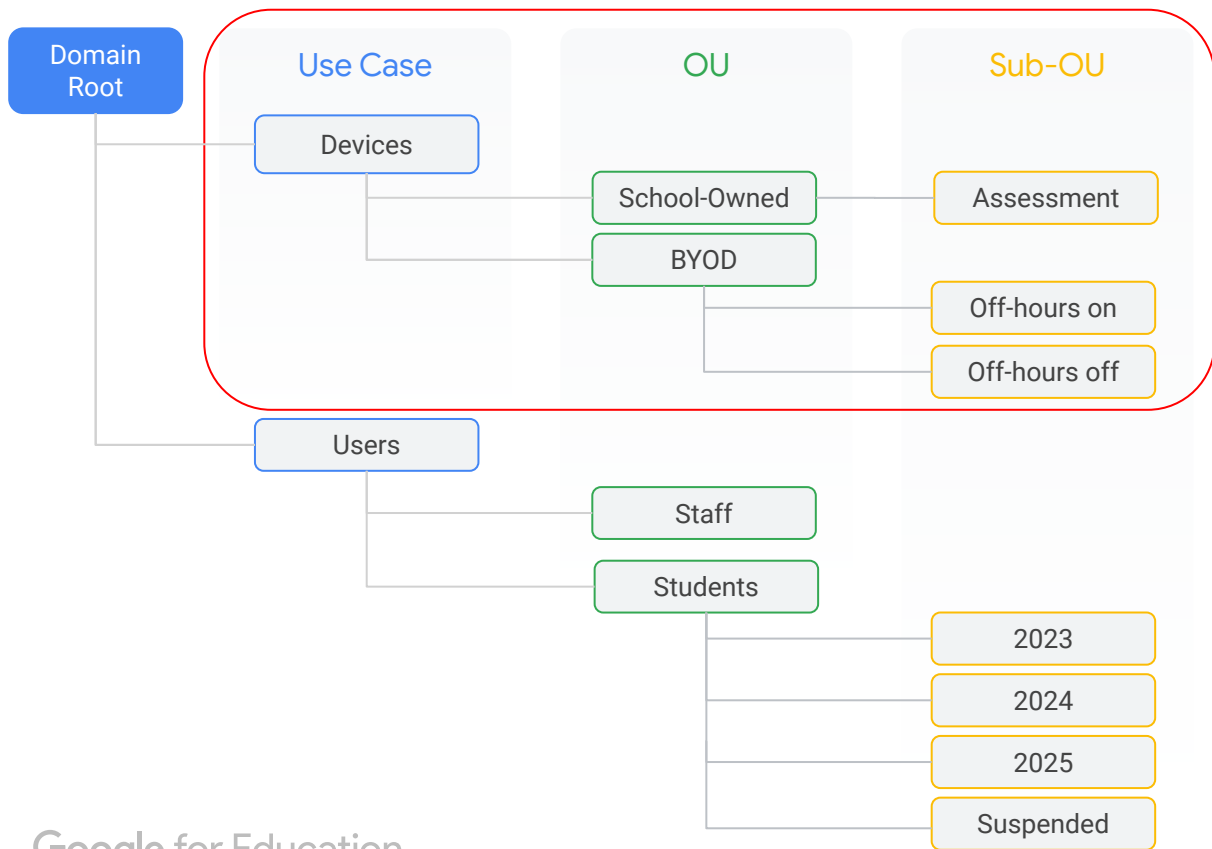
Device settings

Give a custom, school-wide experience on each and every device, no matter who signs in.

Device settings help to maintain control over who can sign in on your Chromebooks. For example, you can create a policy that only users within your domain can sign in.



Recommended Organisational Unit structure



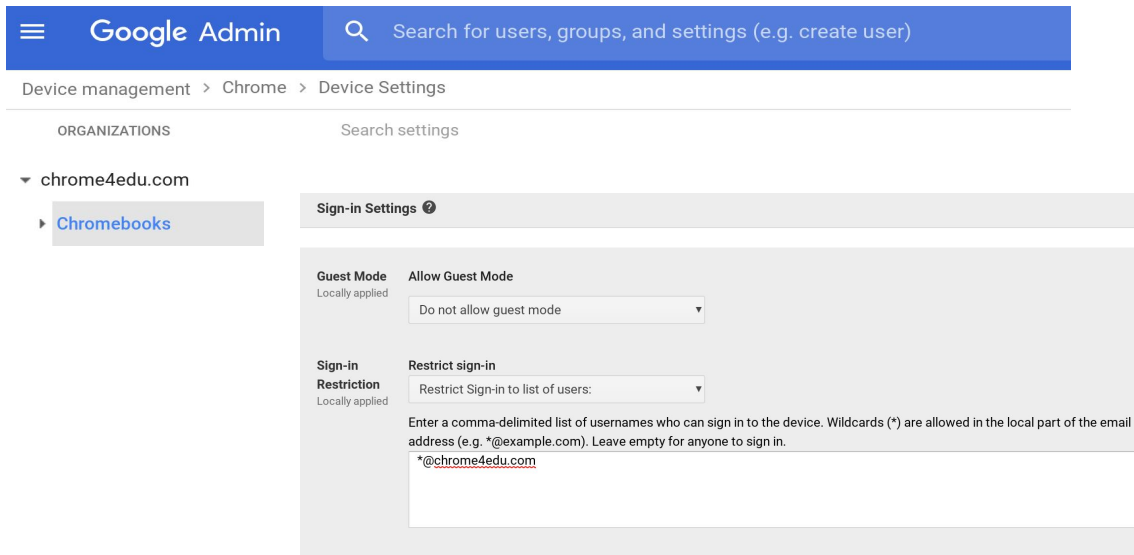
This is an example of how you may want to set up OU's for devices in your organisation. Different settings can be applied for each OU, so devices can be placed in an OU depending on what settings you want them to have.

Note: These OU's show how school's may want to structure their OU's in a BYOD environment - thus utilising the [off-hour sign-in settings](#) that can be applied.

For schools wanting to create a [secure testing](#) environment, you may want to create a Sub-OU called 'Assessment'

Specify who can sign in

Ensure school-owned Chromebooks are only used for educational purposes by disabling guest mode and restricting sign in to your domain.



The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is: Device management > Chrome > Device Settings. The left sidebar shows the 'chrome4edu.com' organization with 'Chromebooks' selected. The main content area displays the 'Sign-in Settings' for Chromebooks. It includes two sections: 'Guest Mode' with 'Allow Guest Mode' set to 'Do not allow guest mode', and 'Sign-in Restriction' with 'Restrict sign-in' set to 'Restrict Sign-in to list of users:'. Below these sections, there is a text box containing the email address '*@chrome4edu.com'.

Guest Mode: Controls whether to allow guest browsing on managed Chrome devices. If you select Allow guest mode (the default), the main sign-in screen offers the option for a user to sign in as a guest. If you select Do not allow guest mode, a user must sign in using a Google Account or G Suite account. When a user signs in using guest mode, your organization's policies are not applied. **For schools, we recommend the "Do not allow guest mode" option.**

Sign-in Restriction: This setting enables you to control which users have permission to sign in to a managed Chrome device. When the default Restrict Sign-in to list of users is selected, and the textbox is left empty, any user with a Google Account or G Suite account can sign in. However, if you include one or more user names in the text box, *only* the named users can sign in; other users will receive an error message. The names can include the wildcard * followed by the domain name, to allow all users within a domain log-in to the Chromebook. **We recommend locking the device to users of your domain, therefore user policies set within that domain are enforced.**

Autocomplete Domain

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is "Device management > Chrome > Device Settings". The main content area is divided into two columns: "ORGANIZATIONS" on the left and "Search settings" on the right. Under "ORGANIZATIONS", "chrome4edu.com" is expanded to show "Chromebooks". The "Search settings" column shows the "Autocomplete Domain" setting, which is "Domain name autocomplete at sign in". The setting is "Locally applied" and has a dropdown menu set to "Use the domain name, set below, for autocomplete". Below this, a text input field shows "username@chrome4edu.com".

Autocomplete Domain: The Domain name autocomplete at sign in setting enables you to choose a domain name to present to users on their sign-in page. When you enable this setting, users don't need to type the *@domain.com* part of their username during sign in. **We recommend enabling this for your school domain to speed up the sign-in process.**

Note: You can override this setting by typing your full username when you sign in.

Off-Hours Sign in Settings

The screenshot shows the Google Admin console interface. At the top, there is a navigation bar with the Google Admin logo and a search bar. Below this, the breadcrumb trail reads "Device management > Chrome > Device Settings". The main content area is titled "ORGANIZATIONS" and "Search settings". Under "ORGANIZATIONS", there is a list of organizations, with "chrome4edu.com" selected. Under "chrome4edu.com", there is a list of device types: "Chromebooks", "BYOD (off-hours off)", "BYOD (off-hours on)" (highlighted in blue), and "School owned". The "BYOD (off-hours on)" option is selected, and its settings are displayed. The settings include "Off Hours" (Locally applied) and "Set hours during which some sign-in restrictions won't apply." A note states: "Note: users who do not meet your regular sign-in criteria must connect to the internet before logging in." Below the note, there is a dropdown menu for the time zone, currently set to "GMT+13:00 New Zealand Time (New Zealand T)". A table of settings follows, with columns for Day, Start Time, End Time, and a trash icon. The table shows the following settings:

Day	Start Time	End Time	Trash Icon
Monday	3:30 PM	Tuesday 8:00 AM	🗑️
Tuesday	3:30 PM	Wednesday 8:00 AM	🗑️
Wednesday	3:30 PM	Thursday 8:00 AM	🗑️
Thursday	3:30 PM	Friday 8:00 AM	🗑️
Friday	3:30 PM	Monday 8:00 AM	🗑️

Below the table, there is a link: "Add another set of hours".

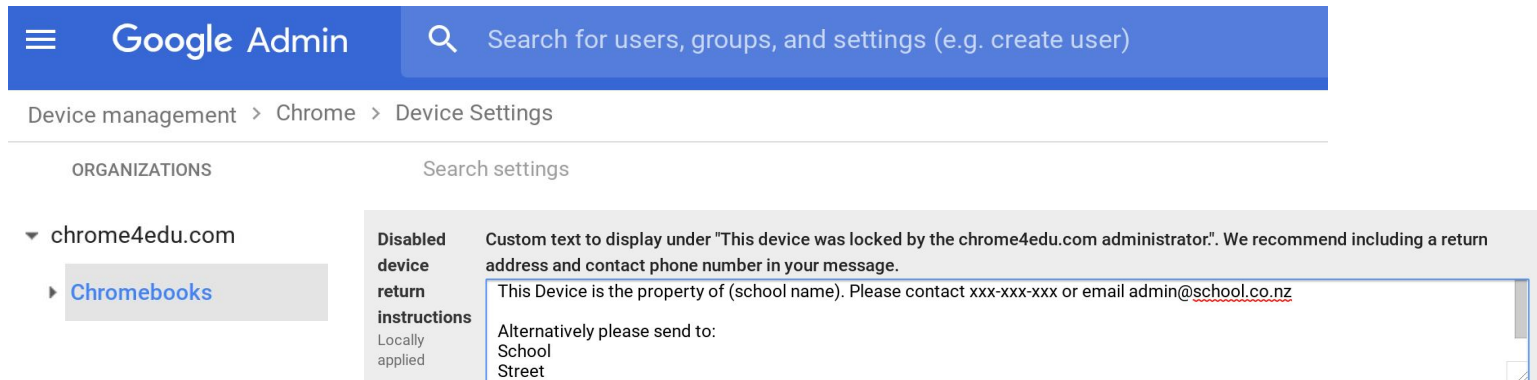
Note: For 'off-hours on' OU's, admin's should set reminders for holidays to allow Guest Mode and allow anyone to sign in. These should be turned off again when school begins and the normal off-hours settings will resume.

Allows you to set a weekly schedule when the guest browsing and sign-in restriction settings don't apply to managed devices running Chrome OS.

For example, school admins can block guest browsing or only allow users with a username ending in `@domain.school.nz` to sign in during school hours. Outside of school hours, users can browse in guest mode or sign in to their device using an account other than their `@domain.school.nz`

For BYO devices, we recommend giving parents the option as to whether or not they want their child's device to have access to the off-hours sign in settings. See the organisational structure on the left to see how this could be applied.

Disabled Device Return Instructions



The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is 'Device management > Chrome > Device Settings'. The main content area is divided into two sections: 'ORGANIZATIONS' and 'Search settings'. Under 'ORGANIZATIONS', 'chrome4edu.com' is expanded to show 'Chromebooks'. The 'Disabled device return instructions' setting is selected, showing a text input field with the following content: 'This Device is the property of (school name). Please contact xxx-xxx-xxx or email admin@school.co.nz'. Below the input field, there is a section for 'Alternatively please send to:' with fields for 'School' and 'Street'.

Device management > Chrome > Device Settings

ORGANIZATIONS Search settings

▼ chrome4edu.com

- ▶ Chromebooks

Disabled device return instructions
Locally applied

Custom text to display under "This device was locked by the chrome4edu.com administrator". We recommend including a return address and contact phone number in your message.

This Device is the property of (school name). Please contact xxx-xxx-xxx or email admin@school.co.nz

Alternatively please send to:
School
Street

This setting controls the custom text on the disabled device screen. **We recommend you include a return address and contact phone number in your message so that users who see this screen are able to return the device to your organisation.** [Click here to see how to disable a device.](#)

Sign-in Keyboard

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is "Device management > Chrome > Device Settings". The main content area is divided into two sections: "ORGANIZATIONS" on the left and "Search settings" on the right. Under "ORGANIZATIONS", "chrome4edu.com" is expanded to show "Chromebooks". The "Sign-in Keyboard" setting is selected, with the subtitle "Locally applied". The main content area is titled "Create an ordered list of keyboards to use on the sign-in screen". It features a "Filter keyboard layouts" search box and a list of keyboard options with checkboxes. The "US keyboard" option is checked. To the right of the list is a "Selected layouts" box containing "US keyboard".

Google Admin

Search for users, groups, and settings (e.g. create user)

Device management > Chrome > Device Settings

ORGANIZATIONS

Search settings

chrome4edu.com

Chromebooks

Sign-in Keyboard
Locally applied

Create an ordered list of keyboards to use on the sign-in screen

Filter keyboard layouts

- US Workman keyboard
- US Workman international keyboard
- US Programmer Dvorak keyboard
- US keyboard [Malay - Melayu]
- US keyboard [Indonesian - Indonesia]
- US keyboard [Filipino]
- US keyboard
- US International keyboard
- US International keyboard
- US Extended keyboard

Selected layouts

US keyboard

Specifies which keyboard layouts are allowed on the Chrome device's sign-in screen.

On shared devices, we recommend choosing one sign keyboard layout to stop students changing the layout so the next person struggles to sign-in.... (i.e the @ button is now no longer where you would expect)

Secure Assessments

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is 'Device management > Chrome > Device Settings'. The left sidebar shows the organizational structure: 'ORGANIZATIONS' with 'chrome4edu.com' expanded to show 'Chromebooks', 'BYOD', and 'School owned'. Under 'School owned', the 'Assessment' option is highlighted. The main content area is titled 'Kiosk Settings' and contains two sections: 'Kiosk Settings' and 'Kiosk Apps'. The 'Kiosk Settings' section has a 'Public Session Kiosk' dropdown set to 'Do not allow Public Session Kiosk' and an 'Auto-Launch Kiosk App' dropdown set to 'None'. The 'Kiosk Apps' section shows 'No kiosk apps available to launch' with a link to 'Manage Kiosk Applications' and a note that 'Android kiosk is officially supported only on certain devices'.

Google Admin

Search for users, groups, and settings (e.g. create user)

Device management > Chrome > Device Settings

ORGANIZATIONS

Search settings

chrome4edu.com

Chromebooks

BYOD

School owned

Assessment

Kiosk Settings

Kiosk Settings
Inherited

Public Session Kiosk
Do not allow Public Session Kiosk

Auto-Launch Kiosk App
None

Kiosk Apps
Inherited

No kiosk apps available to launch [Manage Kiosk Applications](#)

Note: Android kiosk is officially supported only on certain [devices](#)

Chromebooks are a secure platform for administering student assessments. With Chromebooks, you can disable students' access to browse the web during an exam in addition to disabling external storage, screenshots, and the ability to print. Chromebooks can be setup using '[Single App Kiosk](#)' for secure testing.

Secure Assessments: Single App Kiosk

The screenshot shows the Google Admin console interface. At the top, there is a navigation bar with the Google Admin logo and a search bar. Below this, the breadcrumb trail reads "Device management > Chrome > Device Settings". The left sidebar shows the organizational structure for "chrome4edu.com", including "Chromebooks", "BYOD", and "School owned". Under "School owned", the "Assessment" category is highlighted. The main content area displays the "Kiosk Apps" settings. It shows a status message: "No kiosk apps available to launch" with a link to "Manage Kiosk Applications". Below this, it says "Note: Android kiosk is officially supported only on certain devices" and "Inherited". A red box highlights the "Kiosk Apps" section, which contains a list of app sources: "Chrome Web Store", "Domain Apps", "Specify a Custom App", and "Managed Google Play". To the right of this list, there is a summary box showing "Total to install: 1" and a status "NAP: NAP Locked down..." with "Details" and "Remove" links. A red arrow points from the "Manage Kiosk Applications" link to the "Kiosk Apps" section.

Requirement: You need to have the test available as a Chrome kiosk app

Manage Kiosk Apps

1. Go to Device management > Chrome management > Device settings > Kiosk Apps. Click on Manage Kiosk Applications.
2. In the dialog that appears select the exam kiosk app you want to use. You can search for it on the Chrome Web Store, or manually install it if you have the app ID and URL by selecting Specify a Custom App.
3. On the same Device settings page, under Kiosk Settings > Auto-Launch Kiosk App, select the app.
4. Make sure the devices you want to administer the test with are under the organizational unit you select for the kiosk app.

Auto-Launch Setting for a Kiosk App

If Auto-Launch Kiosk App is *not* configured, then the student will see a menu of kiosk apps in the system tray on the login screen. The student needs to select the appropriate kiosk app to launch it in order to take the test. After the test is complete, the student can exit the kiosk app and log back into a user session.

If Auto-Launch Kiosk App is configured, when the device next boots, it will immediately load the kiosk app.

Public Sessions

With public sessions, multiple users can share the same Chrome device without the need to sign in. For example, use public sessions to configure Chrome devices for use as kiosks, loaner devices, shared computers, assessments, libraries, kindergartens or for any other work or school-related purpose for which users don't need to sign in.

1. Go to Device management > Chrome management > Public session settings.
2. Select the OU for which you want the settings to apply.
3. Configure the settings on the page and include a Session Display Name that you would like to appear on the device's home screen, such as the name of your school or the name of a test.
4. Click Save changes.
5. Go to Device management > Chrome management > Device settings.
6. Select the organization you want to configure and under Kiosk Settings > Public Session Kiosk, select Allow Public Session Kiosk. This attaches the public session settings to the devices in the organization you select.
7. Click Save changes. Settings typically take effect within minutes, but they might take up to an hour to propagate to the devices.
8. Move the desired Chrome devices into the OU that that has the public session settings applied.

If you set Auto-Launch Public Session to Yes and enter 0 into the field Number of seconds before delaying auto-login, the device will be a Public Session Kiosk after you logout and go to the sign-in screen. If you want to launch a Chrome device with a single Chrome app full-screen, see how to set up a [Single App Kiosk](#)

User Settings



Note: General information within this section has come from [Google's Device User Settings Support Website](#). Any recommendations are what The Warehouse Group Business consider best practice for NZ schools.

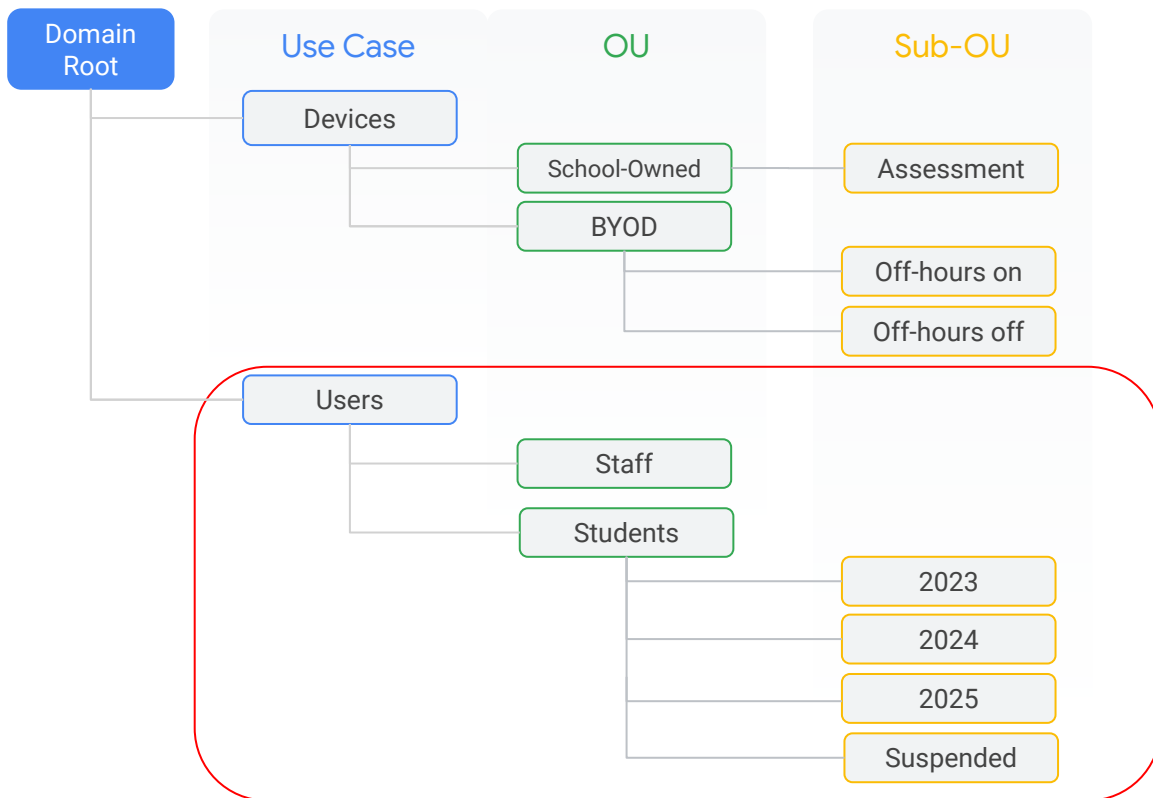
User settings

Create a personalised experience for users on each and every device in your domain, and Chrome browsers everywhere.

User settings are the things the students can take with them no matter what tool or what device they're using.



Recommended Organisational Unit structure



This is an example of how you may want to set up OU's for users in your organisation. Different settings can be applied for each OU, so users can be placed in an OU depending on what settings you want them to have.

For schools wanting to setup public sessions for testing, you may want to create a Sub OU called "Testing" that you can move students in and out of.

Tip: It will save you time at the end or beginning of each year if you name each sub-OU for students according to the year that would be their last year at your school.

Note: As Google for Education accounts have an unlimited amount of users, you may want to consider placing users such as students and staff that have left your school into the an OU for 'Suspended' users rather than deleting them. That way, users can be enabled easily again if needed. After a certain time frame they could be deleted.

Custom Wallpaper

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is "Device management > Chrome > User Settings". On the left side, there is a sidebar with "ORGANIZATIONS" and a list of users: "Staff" and "Students" (selected). The main content area shows the "Wallpaper" settings, which are "Inherited". The "Custom Wallpaper" section is active, featuring a lightbulb icon and a button labeled "UPLOAD WALLPAPER FILE". Below the button, a note states: "We only support jpg (.jpg or .jpeg) files."

Replaces the default wallpaper with your own custom wallpaper (e.g school logos, school picture etc). You can upload images in JPG format (.jpg or .jpeg files) up to a size of 16 megabytes. Other file types are not supported.

Force- install apps and extensions

The screenshot displays the Google Admin console interface. At the top, the 'Google Admin' header is visible with a search bar for users, groups, and settings. The navigation path is 'Device management > Chrome > User Settings'. On the left, the 'ORGANIZATIONS' section shows 'chrome4edu.com' with sub-entities 'Staff' and 'Students'. The main content area is titled 'Force-installed Apps and Extensions' and shows '2 apps or extensions will be automatically installed.' A note below states: 'Note: To ensure force-installed apps and extensions can't be tampered with, we recommend you disallow developer tools access.' A red box highlights a modal window titled 'Force-installed Apps and Extensions' which contains a 'Chrome Web Store' search bar and a list of two items: 'Screencastify - Sc...' and 'Share to Classroom', each with 'Details' and 'Remove' links. The total count is 'Total to force install: 2'.

Choose which apps and extensions to automatically install on the users' Chrome Browsers or devices that run Chrome OS. The apps appear when users sign in to their managed account. Users can't remove force-installed apps. The items also bypass any list of blocked apps and extensions.

Click 'Manage force-installed apps' to select apps and extensions to force-install.

Allow or Block All Apps and Extensions

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the breadcrumb navigation reads 'Device management > Chrome > User Settings'. On the left side, under 'ORGANIZATIONS', there is a tree view showing 'chrome4edu.com' with sub-items 'Staff' and 'Students'. The 'Students' item is selected. The main content area shows the 'Allow or Block All Apps and Extensions' setting, which is 'Inherited'. The setting description is 'Choose which Chrome apps and extensions to allow.' The current value is 'Allow all apps and extensions except the ones I block', indicated by a dropdown menu and a lightbulb icon.

Select whether you want to allow or block users from installing all apps and extensions. Based on the setting you choose, you can then make exceptions using the Allowed Apps and Extensions setting. If you choose to “Block all apps and extensions except the ones you allow”, the next block lets you choose what apps or extensions will be allowed for your users.

The screenshot shows the 'Allowed Apps and Extensions' setting, which is 'Inherited'. The setting description is '4 apps or extensions are allowed. Manage', with a lightbulb icon next to the 'Manage' link.

Block Extensions by Permission

Google Admin

Search for users, groups, and settings (e.g. manage user data)

Device management > Chrome > User Settings

ORGANIZATIONS

- chrome4edu.com
 - Staff
 - Students

Search settings

Block Extensions by Permission

Permissions and URLs ⓘ

Block extensions by permissions and URLs. [Learn more](#)

Permission: If the extension uses one of the selected permissions, block ▾

Locally applied

<input type="checkbox"/> Alarms	<input type="checkbox"/> Audio Capture	<input type="checkbox"/> Certificate Provider	<input type="checkbox"/> Clipboard Read
<input type="checkbox"/> Clipboard Write	<input type="checkbox"/> Context Menus	<input type="checkbox"/> Desktop Capture	<input type="checkbox"/> Document Scan
<input type="checkbox"/> Enterprise Device Attributes	<input type="checkbox"/> Experimental APIs	<input type="checkbox"/> Fullscreen Apps	<input type="checkbox"/> File Browser Handler
<input type="checkbox"/> File System	<input type="checkbox"/> File System Provider	<input type="checkbox"/> HID	<input type="checkbox"/> Override Fullscreen
<input type="checkbox"/> Detect Idle	<input type="checkbox"/> Identity	<input type="checkbox"/> Google Cloud Messaging Captive Portal	<input type="checkbox"/> Escape Geo Location
<input type="checkbox"/> Media Galleries	<input type="checkbox"/> Native Messaging	<input type="checkbox"/> Authenticator Serial	<input type="checkbox"/> Power
<input type="checkbox"/> Notifications	<input type="checkbox"/> Printers	<input checked="" type="checkbox"/> Set Proxy	
<input type="checkbox"/> Platform Keys	<input type="checkbox"/> Storage	<input type="checkbox"/> Sync File System	<input type="checkbox"/> CPU Metadata
<input type="checkbox"/> Memory Metadata	<input type="checkbox"/> Network Metadata	<input type="checkbox"/> Display Metadata	<input type="checkbox"/> Storage Metadata
<input type="checkbox"/> 2-Factor Devices	<input type="checkbox"/> Text to Speech	<input type="checkbox"/> Unlimited Storage	<input type="checkbox"/> USB
<input type="checkbox"/> Video Capture	<input checked="" type="checkbox"/> VPN Provider	<input type="checkbox"/> Web Requests	<input type="checkbox"/> Block Web Requests

Prevent users from running extensions that request certain permissions that your organization doesn't allow. Select whether to allow or block apps that request specific permissions. Then check the permissions to allow or block.

Pinned Apps and Extensions

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the 'Google Admin' logo and a search bar. Below the header, the navigation path is 'Device management > Chrome > User Settings'. The main content area is divided into two columns. The left column shows a list of organizations, with 'chrome4edu.com' selected and expanded to show 'Staff' and 'Students' (the latter is highlighted). The right column shows the 'Pinned Apps and Extensions' setting, which states: 'Pinned Apps and Extensions 3 apps or extensions will be pinned to the Chrome launcher if they are installed. [Manage pinned apps](#)'. A lightbulb icon is next to the link.

This screenshot shows a configuration window titled 'Pinned Apps and Extensions'. It contains the following information:

- Title:** Pinned Apps and Extensions
- Message:** The selected apps and extensions will be pinned to the Chrome launcher.
- Source:** Chrome Web Store (with a back arrow and search bar)
- Total to pin:** 3
- Selected Apps:**
 - Google Classroom (Details Remove)
 - Google Drive (Details Remove)
 - Gmail (Details Remove)

This setting pins the apps and extensions pinned to the app launcher that your users see when signed in to their Chrome device.

This policy has no effect on Android apps running on Chrome OS. For information on force installing Android apps on Chrome devices that support them, see 'Installing Android Apps'

Chrome Web Store

Google Admin Search for users, groups, and settings (e.g. manage user data)

Device management > Chrome > User Settings

ORGANIZATIONS

- chrome4edu.com
 - Staff
 - Students

Search settings

Chrome Web Store ⓘ

Chrome Web Store Homepage
Use the "For chrome4edu.com" collection:
https://chrome.google.com/webstore/category/for_your_domain







"For chrome4edu.com" Collection
You may recommend apps and extensions for your domain in a custom collection in Chrome Web Store.
5 apps or extensions are recommended for your users. [Manage](#)

Recommended Apps and Extensions
Inherited

You can change the Chrome Web Store Homepage to a custom homepage for your users when they're signed in. You can also recommend apps and extensions for your domain in a custom collection named after your domain in the Chrome Web Store.

Recommended apps and extensions

The selected apps and extensions will appear in the "For chrome4edu.com" collection.

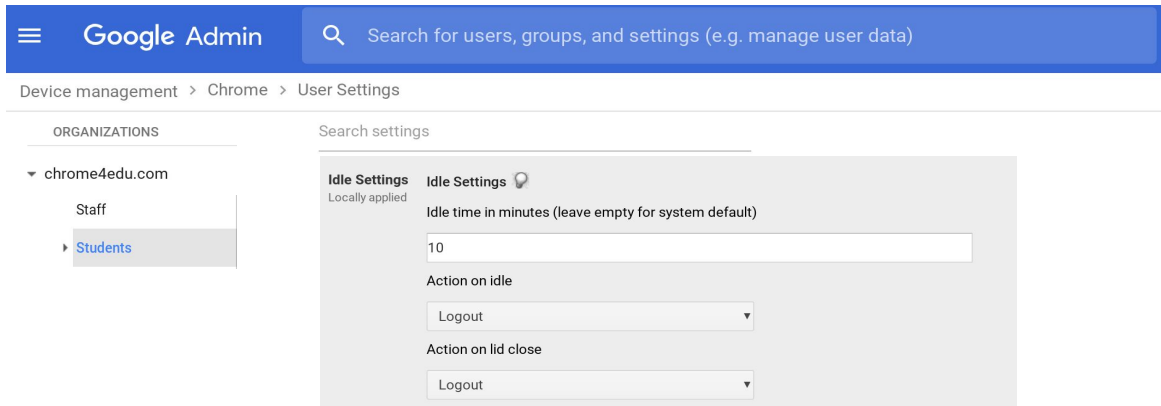
Total to recommend: 4	
 Chrome Web Store >	Details Remove Inherited
 Domain Apps >	
 Tynker for Educat...	Details Remove Inherited
 Khan Academy He...	Details Remove Inherited
 Quizlet	Details Remove Inherited
 Read&Write for G...	Details Remove Inherited

Android Applications on Chrome Devices

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the breadcrumb navigation reads 'Device management > Chrome > User Settings'. On the left side, there is a sidebar with 'ORGANIZATIONS' and a list of users: 'Staff' and 'Students'. The 'Students' user is selected. The main content area shows the 'Android applications' policy. The policy is titled 'Android applications on Chrome Devices' and is currently set to 'Inherited'. The policy description states: 'Allow an approved set of Android applications to be installed on supported Chrome Devices'. A note below the description says: 'Note: Android apps on Chromebooks are available as a beta feature for Chrome Education customers.' Below the note is a dropdown menu currently set to 'Allow'. Further down, there is a warning message: 'Please read this article before enabling this policy. This policy is only supported on certain devices, and if those devices are older, they will require a file system migration before this policy will take effect. Learn more. We also recommend you configure applications in the App Management section before enabling this policy so users have applications to use. Learn more.'

By default, users in this organization are not allowed to install Android Apps on devices. Selecting Allow will give users access to the approved apps in the Google Play Store on their Chrome devices. (Note: only approved apps will be available, see [Android Apps](#) and not all Chromebooks are capable of running Android Apps)

Idle Settings



The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is "Device management > Chrome > User Settings". On the left side, there is a sidebar with "ORGANIZATIONS" and a tree view showing "chrome4edu.com" with sub-items "Staff" and "Students". The main content area is titled "Search settings" and displays the "Idle Settings" configuration for a user. The settings are "Locally applied" and include: "Idle time in minutes (leave empty for system default)" with a text input field containing "10"; "Action on idle" with a dropdown menu set to "Logout"; and "Action on lid close" with a dropdown menu set to "Logout".

Idle time in minutes

To specify the amount of idle time before a user's device goes to sleep or signs them out, enter a value in minutes. To use the system default, which varies by device, leave the box empty.

Action on idle

Select what you want the device to do after the idle time expires:

- Sleep—if you want the device to go into sleep mode
- Logout—if you want to sign out the current user
- Lock Screen—if you want to lock the screen on the users device without signing them out

Action on lid close

Select if you want a user's device to go to sleep or sign them out when they close the device lid. **On shared devices, we recommend the 'logout' on lid close option as this will keep users data safe if they forget to sign out of the device when they return it.**

Incognito Mode and Browser History

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is "Device management > Chrome > User Settings". On the left, there is a sidebar with "ORGANIZATIONS" and a list of users under "chrome4edu.com", including "Staff" and "Students". The main content area displays three settings cards:

- Incognito Mode:** Labeled "Locally applied", with a dropdown menu set to "Disallow incognito mode".
- Browser History:** Labeled "Inherited", with a dropdown menu set to "Always save browser history".
- Clear Browser History:** Labeled "Locally applied", with a dropdown menu set to "Do not allow clearing history in settings menu".

Incognito Mode: Setting this policy to Disallow Incognito Mode prevents users from opening new incognito windows. ***We recommend this for students to ensure that user settings stay in place.***

Browser History: Controls whether the browser saves the user's browsing history. ***We recommend 'always saving browser history' so teachers can view what sites students have visited.***

Clear Browser History: Specifies whether users can clear browser data, including their browsing and download history. ***We recommend 'Do not allow clearing of history in settings menu' so teachers can view what sites students have visited without students deleting it.***

Safe Browsing

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is 'Device management > Chrome > User Settings'. On the left side, under 'ORGANIZATIONS', there is a tree view showing 'chrome4edu.com' with sub-items 'Staff' and 'Students'. The 'Students' item is selected. The main content area shows the 'Safe Browsing' setting, which is 'Locally applied' and set to 'Always enable Safe Browsing'.

Safe Browsing in Chrome helps protect users from websites that may contain malware or phishing content.

The default setting is Allow user to decide whether to use Safe Browsing. ***We recommend the setting 'Always enable Safe Browsing' for your users.***

Homepage and Pages to Load on Startup

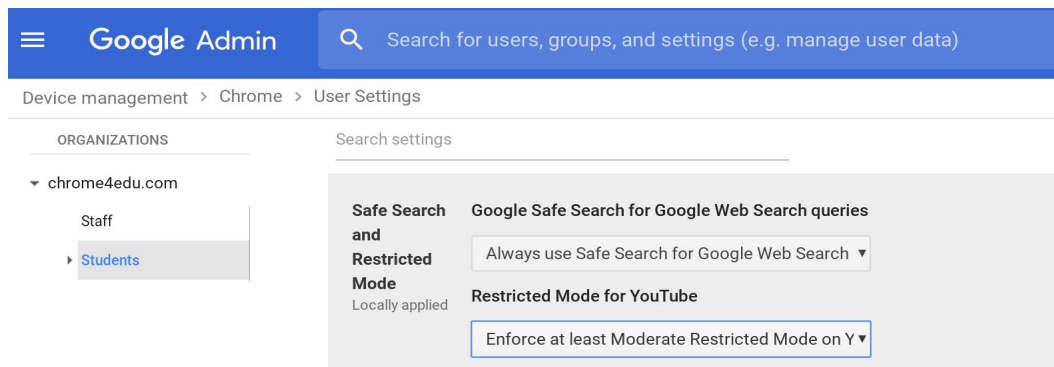
The screenshot shows the Google Admin console interface. At the top, there is a blue header with the 'Google Admin' logo and a search bar containing the text 'Search for users, groups, and settings (e.g. manage user data)'. Below the header, the navigation path is 'Device management > Chrome > User Settings'. On the left side, under 'ORGANIZATIONS', there is a tree view showing 'chrome4edu.com' with sub-items 'Staff' and 'Students'. The 'Students' item is selected. The main content area is titled 'Search settings' and displays the 'Homepage' settings for the selected group. The 'Homepage' section has a sub-header 'Homepage is New Tab Page' and a dropdown menu set to 'Homepage is always the Homepage URL, set below'. Below this is a text input field containing 'www.school.co.nz'. The 'Pages to Load on Startup' section has a sub-header 'Pages to Load on Startup' and a note: 'Put each URL on its own line. For example: example.org'. Below this is a text input field containing two lines: 'https://drive.google.com' and 'https://classroom.google.com/'.

Homepage: The default is to Allow user to configure their new homepage in their Chrome menu . If you don't want to allow the user to change the homepage, you can specify that the Homepage is always the new tab page or that the Home page is always the Homepage URL, set below.

If you select Homepage is always the Homepage URL, set below, enter the URL for the homepage in the text box. With this option, users can't change their homepage in Chrome.

Pages to Load on Startup: Enables you to specify URLs for pages that should load when the user starts the Chrome device. The specified home page appears on the active tab; any pages you list here appear on additional tabs.

Safe Search and YouTube Restricted Mode



The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is "Device management > Chrome > User Settings". The main content area is titled "Search settings" and is divided into two sections: "ORGANIZATIONS" and "Search settings". Under "ORGANIZATIONS", there is a list of organizations including "chrome4edu.com" with sub-groups "Staff" and "Students". The "Students" group is selected. The "Search settings" section contains two settings: "Safe Search and Restricted Mode" (Locally applied) and "Google Safe Search for Google Web Search queries" (Always use Safe Search for Google Web Search). Below this, there is a section for "Restricted Mode for YouTube" with a dropdown menu set to "Enforce at least Moderate Restricted Mode on Y".

Google Safe Search for Google Web Search queries

- **Do not enforce Safe Search for Google Web Search queries** - Default setting.
- **Always use Safe Search for Google Web Search queries** - Selecting this option will make your selected users use SafeSearch. *We recommend this setting for your students.*

Restricted Mode for YouTube

- **Do not enforce Restricted Mode on YouTube** - Default setting.
- **Enforce at least Moderate Restricted Mode on YouTube** - Selecting this option will make your selected users use Restricted Mode. It limits which videos are viewable based on their content and also blocks the comments.
- **Enforce Strict Restricted Mode for YouTube** - Selecting this option will make your selected users use Strict Restricted Mode. This further limits available videos.

We recommend enforcing either moderate or strict restricted mode on for your students

URL Blocking

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is "Device management > Chrome > User Settings". The main content area is divided into two columns. The left column, titled "ORGANIZATIONS", shows a tree view with "chrome4edu.com" expanded to show "Staff" and "Students". The right column, titled "Search settings", shows the "URL Blocking" policy. The policy is described as "URL Blacklist" and "Locally applied". The description states: "Any URL in the URL blacklist will be blocked, unless it also appears in the URL blacklist exception list. Put each URL on its own line. For example: example.org http://example.com [Google Chrome Build 15.0.874.12+]". Below the description is a text input field containing the URLs "facebook.com" and "snapchat.com".

URL Blacklist: Prevents Chrome users from accessing specific URLs.

To configure this policy, enter up to 1,000 URLs on separate lines.

Managed Bookmarks

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is "Device management > Chrome > User Settings". The left sidebar shows the "ORGANIZATIONS" section with "chrome4edu.com" expanded to show "Staff" and "Students". The main content area is titled "Search settings" and displays the "Managed Bookmarks" settings for a "Locally applied" policy. The settings include a "Managed Bookmarks Folder Name" field with the value "Useful Links". Below this is a table of "Managed Bookmarks" with 3 items. The table has columns for "URL", "Name", and "Count".

URL	Name	Count: 3
https://classroom.google.com	Classroom	
https://edutraincenter.withgoogle.c	Google training Centre	
https://www.google.com/intl/en_uk/ec	Google for Education - Computer Science	
<input type="text" value="www.example.com"/>	<input type="text" value="Name"/>	

Allows you to push a list of bookmarks for the convenience of users on Chrome on all platforms including mobile devices.

Note: You can only create one folder of managed bookmarks, so we suggest giving the folder a generic name (e.g Useful Links or School Links etc).

Download Location

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is 'Device management > Chrome > User Settings'. On the left side, there is a sidebar with 'ORGANIZATIONS' and a list of users: 'Staff' and 'Students' (selected). The main content area shows the 'Download Location' setting, which is 'Locally applied'. The 'Set download location' dropdown menu is open, showing 'Force Google Drive' as the selected option.

Sets the default download location on Chrome devices and specifies whether a user is allowed to modify that location. The download location policy choices are:

- **Set Google Drive as default, but allow user to change**
- **Local Downloads folder, but allow user to change**
- **Force Google Drive**

If you select Force Google Drive (regardless of prior user choice), Google Drive is forced to be the download folder and a user is not allowed to change this setting. However, the user can still move files between local folders and Google Drive using the Files app.

For G Suite for Education users, and especially those using shared devices, we recommend the 'Force Google Drive' option.

Disable Hardware

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is 'Device management > Chrome > User Settings'. On the left side, there is a sidebar with 'ORGANIZATIONS' and a tree view showing 'chrome4edu.com' with sub-items 'Staff' and 'Students'. The main content area is titled 'Hardware' and contains a search bar and four settings sections: 'External Storage Devices' (Secure Digital (SD) Cards, USB Flash Drive Devices, and MTP devices), 'Audio Input' (Microphone and Audio Input), 'Audio Output' (Speakers and Audio Output), and 'Video Input' (Video Input). Each section has a dropdown menu to select a policy.

Google Admin

Search for users, groups, and settings (e.g. manage user data)

Device management > Chrome > User Settings

ORGANIZATIONS

chrome4edu.com

- Staff
- Students

Search settings

Hardware

External Storage Devices
Inherited

Secure Digital (SD) Cards, USB Flash Drive Devices, and MTP devices

Allow external storage devices

Audio Input
Inherited

Microphone and Audio Input

Prompt user to allow each time

Audio Output
Inherited

Speakers and Audio Output

Enable audio output

Video Input
Inherited

Video Input

Enable video input

External Storage devices: Controls whether users in your organization can use Chrome devices to mount external drives, including USB flash drives, external hard drives, optical storage, Secure Digital (SD) cards, and other memory cards.

Audio Input: Controls whether users in your organization can let websites access audio input from the built-in microphone on a Chrome device.

This policy does not affect input from external audio input devices, such as microphones that users connect to the USB port. When a user connects an external audio input device, the audio on the Chrome device unmutes immediately.

Audio Output: Controls whether users in your organization can play sound on their Chrome devices. The policy applies to all audio outputs on Chrome devices, including built-in speakers, headphone jacks, and external devices attached to HDMI and USB ports.

Video Input: Specifies whether websites can access the built-in Chrome device webcam.

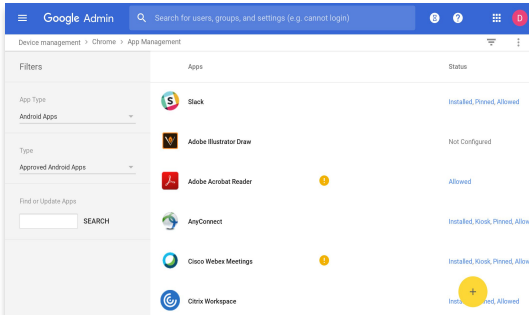
Android Apps Google Play



Note: General information within this section has come from [Google's Android apps on Chrome devices Support Website](#). Any recommendations are what The Warehouse Group Business consider best practice for NZ schools.

Android on Chrome Administration

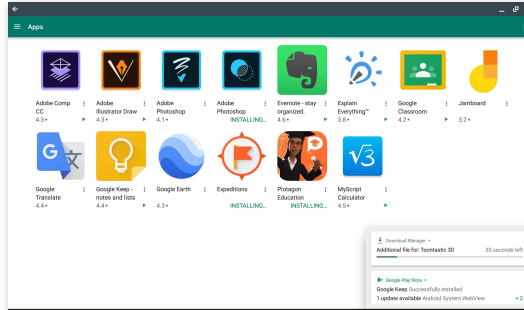
App management



The screenshot shows the Google Admin console interface for App Management. On the left, there are filters for App Type (Android Apps), Type (Approved Android Apps), and a search bar. The main area displays a list of installed apps with columns for App Name, Status, and a plus icon for more options. Visible apps include Slack, Adobe Illustrator Draw, Adobe Acrobat Reader, AnyConnect, Cisco Webex Meetings, and Citrix Workspace.

Allow install, force install, pin to taskbar

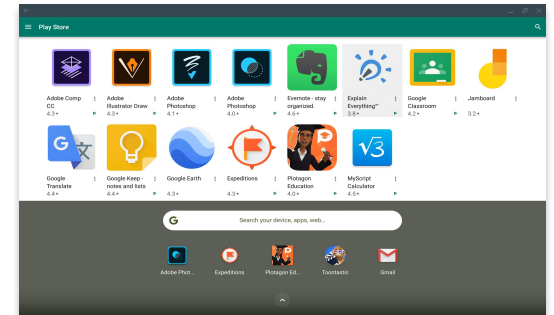
School approved apps available for download by students or force-installed for users



The screenshot shows an Android phone home screen with a grid of app icons. A notification banner at the bottom indicates that Google Keep has been successfully installed. The taskbar at the bottom shows various system icons and the time 9:36 AM.

App sync and install

Automatically syncs when students log in for the first time



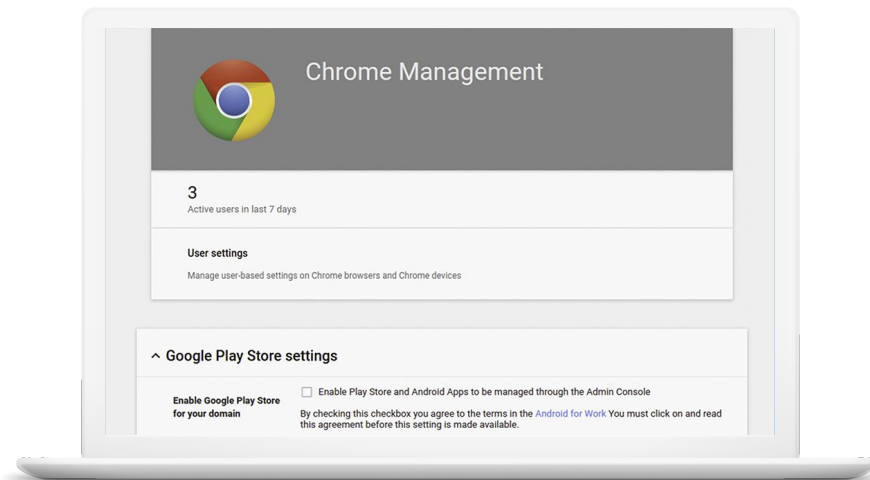
The screenshot shows an Android phone home screen with a grid of app icons. A notification banner at the bottom indicates that Google Keep has been successfully installed. The taskbar at the bottom shows various system icons and the time 9:41 AM.

School approved, managed library

Managed through Admin Console; select from top EDU apps; configure to OU; push or allow install

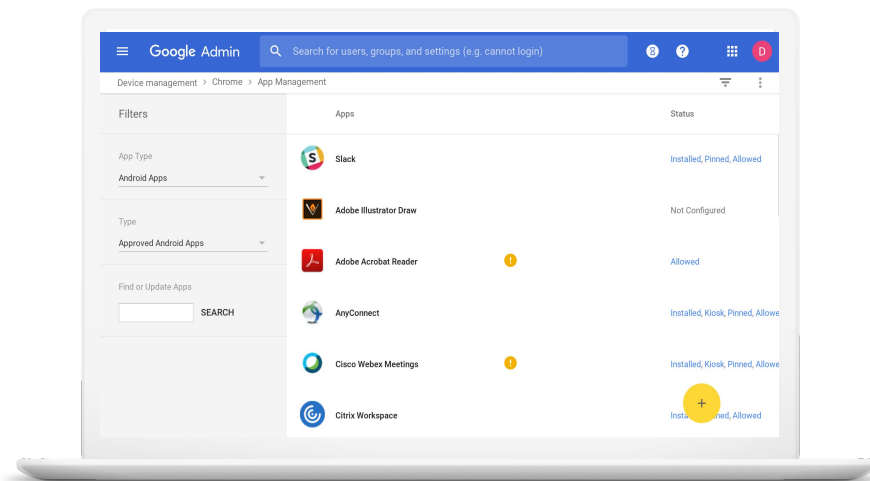
Google Play Store and Admin Console

- Disabled by default for managed devices
- Enable in Admin Console for the domain:
 - Device Management > Chrome Management > Android Application Settings
- The Play Store on Chromebooks needs to be allowed at OU level via user policy



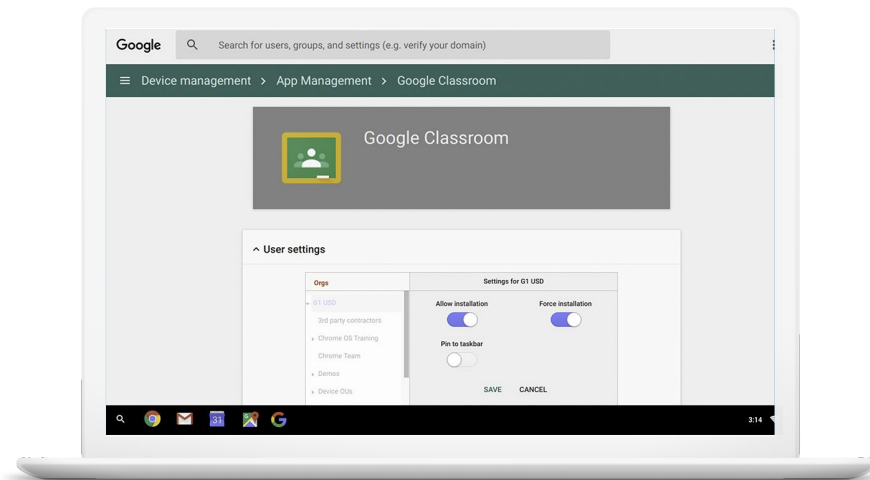
Approving Android Apps

- Android apps need to be approved before they can be installed
 - Go to Device management > Chrome > App Management
 - Choose Android Apps under App Type
 - Click the yellow + to open Google Play
 - Search for the required App
 - Click Approve
 - Review permissions
 - Click Approve
 - Choose between accepting new permissions or revoking approval if permissions change



App Management

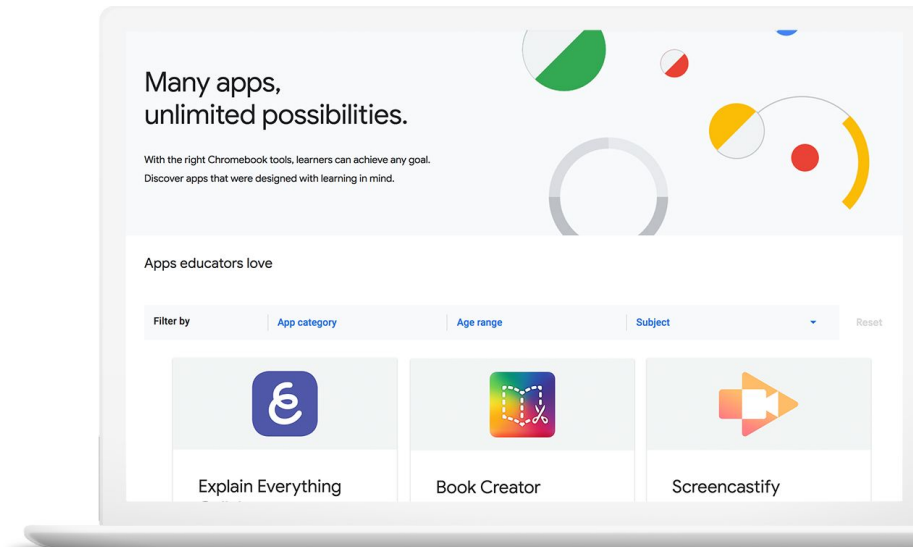
- Approved apps are available to all users in the domain to allow or force installation.
- Select app and manage assignment by OU (same as any Chrome apps)
 - Allow installation
 - Force install
 - Pin to taskbar



Chromebook App Hub

A **platform** to enable educators and developers to work together in order to showcase **Chromebook apps** and to **engage Chromebook activity ideas** for classroom.

chromebookapphub.withgoogle.com



Devices



Note: General information within this section has come from [Google's Manage policies for Chrome devices website](#). Any recommendations are what The Warehouse Group Business consider best practice for NZ schools.

Devices

See all the devices logged into your domain. Looking for something specific? Just sort and filter the list.

The primary use for this has to do with inventory. You can see where devices should be located, what the serial number and Asset ID is, disable and deprovision devices, and track recent users.



Device Details

The screenshot shows the Google Admin console interface. At the top, there's a blue header with 'Google Admin' and a search bar. Below the header, the breadcrumb trail reads 'Device management > Chrome > Devices'. A dark grey bar indicates '98 Chrome devices' with a filter for 'Status: Provisioned'. A table lists three devices with columns for Serial number, Status, Asset ID, Organisational unit, Enrolment time, Last policy sync, User, Location, Notes, and Auto-update expiration. A sidebar on the left shows the organizational unit hierarchy for 'gedu.demo.noelleeming.co.nz'.

<input type="checkbox"/>	Serial number	Status	Asset ID	Organisational unit	Enrolment time	Last policy sync ↓	User	Location	Notes	Auto-update expiration	
<input type="checkbox"/>	NXGM8SA0028100DAB97600	Provisioned	C11	Demo Kit C	29 May 2018, 10:33	27 Aug 2019, 17:30	cdemo@gedu.demo.noelleeming.co.nz			Jan 2022	
<input type="checkbox"/>	NXGNJSA00173917E4C7600	Provisioned	C22	Demo Kit C	6 Jul 2018, 12:57	27 Aug 2019, 17:05	cdemo@gedu.demo.noelleeming.co.nz			Nov 2023	
<input type="checkbox"/>	NXGNJSA0017391837E7600	Provisioned	C14	Demo Kit C	29 May 2018, 10:51	27 Aug 2019, 16:45	cdemo@gedu.demo.noelleeming.co.nz			Nov 2023	

In 'Chrome Devices', admin's are able to view the following in regards to each of the managed devices for their organisation: Serial number; Status (i.e provisioned or deprovisioned); Asset ID; Enrollment Date; Last Sync; User; Location; Notes, [Auto-update expiration](#)

The 'user' is initially populated with the user who first enrolled the device. You can edit the field after auto-population.

Note: You can see the Serial Number and Asset ID of a device by pressing **Alt+V** before signing in.

Track Active Times and Recent Users

Device management > Chrome devices > P202CCAV

^ System Activity and Troubleshooting

Active Times ?	Date	Active Time
	Jul 31, 2018	1 minute
	Aug 7, 2018	4 hours 17 minutes
	Aug 8, 2018	2 hours 50 minutes

Recent Users ? (most to least recent)	
	edupartner7@chrome4edu.com
	edupartner23@chrome4edu.com
	edupartner12@chrome4edu.com
	adminlogin1@chrome4edu.com
	edupartner30@chrome4edu.com

In Chrome Devices, locate the device via the Asset ID and click on the corresponding serial number. Scroll to 'System Activity and Troubleshooting' to see Active Times and Recent Users.

Active Times: Shows up to the last 15 days of activity on the device, including when it was last used and for how long. The times and dates shown are based on the time zone of the device. You can turn this feature on in the Admin console at Device management > Chrome management > Device settings > Device State Reporting.

Recent Users: Displays the last users of the Chrome device. Public, kiosk, and guest-mode sessions are not reported. Email addresses for unmanaged users are not displayed; instead these display as "User not managed by your domain". You can turn on this feature in the Admin console at Device management > Chrome management > Device settings > Device Reporting > Device User Tracking.

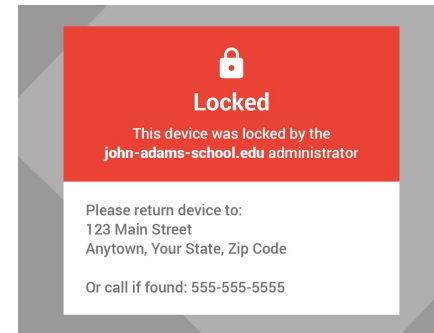
How to disable a device

1. From the Admin console Home page, go to Device management - Chrome devices.
2. If you don't see Device management on the Home page, click More controls at the bottom.
3. If the Filters pane on the left isn't open, click Filter to open it.
4. On the left, under By Status, select Provisioned.
5. On the left, click the organization the device is in.
Tip: If you don't know which organization a device is in, you can search by device serial number or Asset ID in the search field at the top of the list of organizations.
6. Check the box next to the device you want to disable.
7. At the top, click More Actions - Disable.
Note: We recommend that you include a [return address and contact phone number in your message](#). You can edit the message on the device settings page for the device's organizational unit.
8. Click Disable.

Device management > Chrome devices

Filter: Status=Provisioned > Organization=pablotech.com > Coffee Shop Stores

Move to	More Actions	Serial Number	Status	Asset ID	Enrollment Date	Last Sync
<input checked="" type="checkbox"/>	Export MEID List Deprovision Disable Re-enable	9SL...	Provisioned	none specified	Sep 27, 2017 1:38:32 PM	Oct 2, 2017 12:57:06 PM
<input checked="" type="checkbox"/>		5CD...	Provisioned	none specified	Sep 26, 2017 6:14:56 PM	Oct 2, 2017 12:56:53 PM
<input checked="" type="checkbox"/>		1S20GL0005USLR064EMG	Provisioned	none specified	Sep 26, 2017 6:22:19 PM	Sep 28, 2017 4:38:11 PM
<input checked="" type="checkbox"/>		5512000108	Provisioned	none specified	Sep 26, 2017 6:22:47 PM	Sep 27, 2017 3:38:55 PM

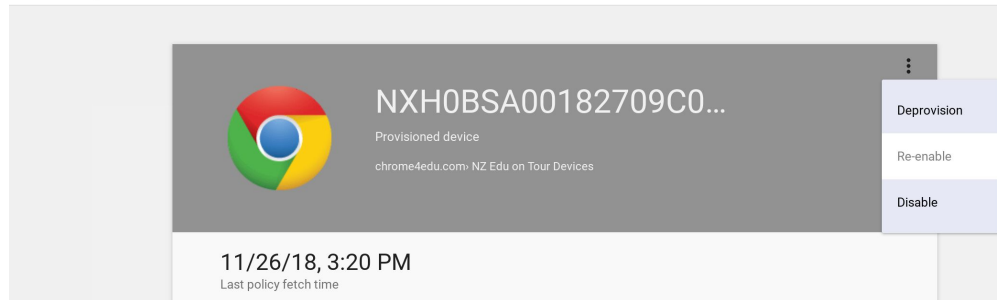


How to deprovision a device

1. From the Admin console Home page, go to Device management - Chrome devices.
2. If you don't see Device management on the Home page, click More controls at the bottom.
3. If the Filters pane on the left isn't open, click Filter to open it.
4. On the left, under By Status, select Provisioned.
5. On the left, click the organization the device is in.
Tip: If you don't know which organization a device is in, you can search by device serial number or Asset ID in the search field at the top of the list of organizations.
6. Check the box next to the device you want to disable.
7. At the top, click More Actions - Disable.
Note: We recommend that you include a [return address and contact phone number in your message](#). You can edit the message on the device settings page for the device's organizational unit.
8. Click Disable.

Note: You can also click on the devices serial number, click on the more actions button and click disable device (as shown on the right).

Device management > Chrome devices > NXH0BSA00182709C0D7600



Note: In a BYOD scenario, when a student leaves your school, you should deprovision the device in the admin console and then physically [wipe the device](#).

How to wipe a device

If a device has been previously enrolled and deprovisioned, you will need to wipe the device so that it can be enrolled onto your domain. To do this, follow the steps below:

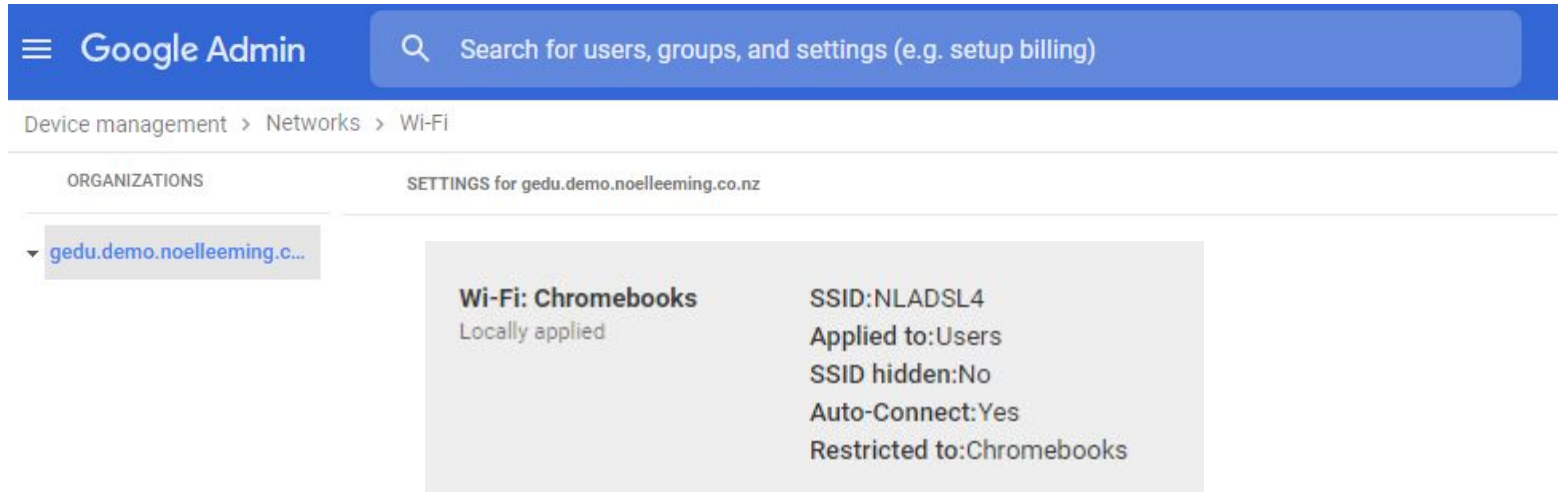
- 1 Press **Esc** + “**refresh**” + **Power**. A yellow exclamation point (!) is displayed.
- 2 Press **Ctrl** + **D** to begin dev mode, then **Enter**.
A red exclamation point is displayed.
- 3 “**OS Verification is OFF**” message is displayed
press Space, then Enter.
- 4 “**OS Verification is now ON**” - device will reboot

Network Settings



Note: General information within this section has come from [Google's Manage networks Support Website](#). Any recommendations are what The Warehouse Group Business consider best practice for NZ schools.

Recommended Wi-Fi Settings



The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is "Device management > Networks > Wi-Fi". The main content area is divided into two sections: "ORGANIZATIONS" on the left and "SETTINGS for gedu.demo.noelleeming.co.nz" on the right. Under "ORGANIZATIONS", the organization "gedu.demo.noelleeming.c..." is selected. The "SETTINGS" section displays a "Wi-Fi: Chromebooks" setting, which is "Locally applied". The settings for this configuration are: SSID: NLADSL4, Applied to: Users, SSID hidden: No, Auto-Connect: Yes, and Restricted to: Chromebooks.

Google Admin

Search for users, groups, and settings (e.g. setup billing)

Device management > Networks > Wi-Fi

ORGANIZATIONS

SETTINGS for gedu.demo.noelleeming.co.nz

gedu.demo.noelleeming.c...

Wi-Fi: Chromebooks
Locally applied

SSID: NLADSL4
Applied to: Users
SSID hidden: No
Auto-Connect: Yes
Restricted to: Chromebooks

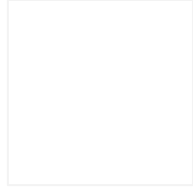
We recommend pushing Wi-Fi settings to your Chromebooks (either via device or user) so that Chromebooks will connect automatically to your network.

Google Vault



Note: General information within this section has come from [Google's Google Vault Support Website](#). Any recommendations are what The Warehouse Group Business consider best practice for NZ schools.

Google Vault



What is Google Vault?

Use Vault to retain, hold, search, and export data in support of your organization's retention and eDiscovery needs.

Vault supports:

- Gmail messages
- Chats in Google Meet with history turned on
- Google Groups
- Files in Google Drive
- Recordings in Google Meet

Recommended Google Vault Retention Policies

We recommend that you should set up retention rules to cover the amount of time data should be retained by your school. You should consult the relevant people at your school to decide on the time-frame that data should be retained.

- In Vault, click Retention in the left navigation.
- Under Default retention rule, click a service, such as Drive or Gmail.
- Check the Set a default retention rule box.
- Choose how long to keep messages or files:
 - Choose Indefinitely to permanently retain data.
 - Click Save to create the default retention rule.
 - Enter a number of days, from 0 to 36,500:
 - Gmail, Groups, and Chat messages—days from when the message was sent.
 - Drive—days from when the file was either created or last modified.
- Choose what to do with data past the duration you selected:
 - Choose the first option to expunge just the messages or files that users have already deleted.
 - Choose the second option to expunge all messages and files. This includes data that's in users' inboxes and Drives. It also includes data that has already been deleted.
- Click Continue.

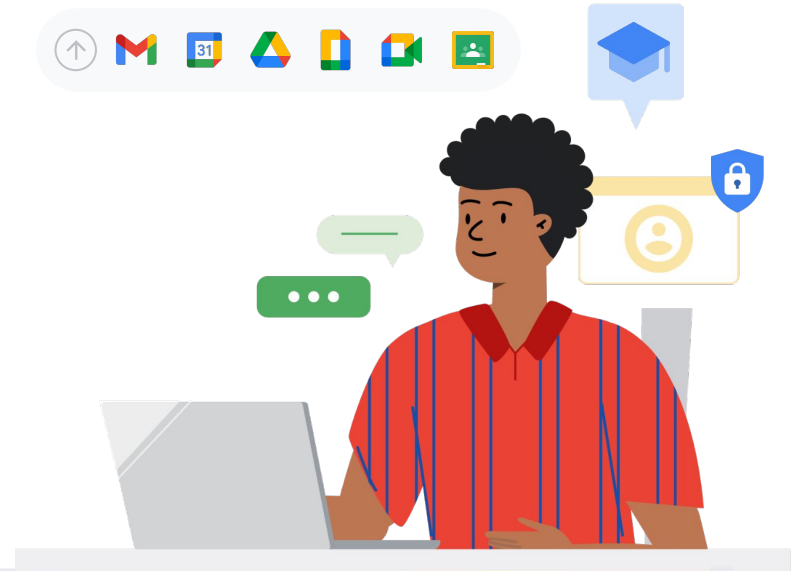
Important notes:

- **What happens after you set default retention rules:** Unless a custom rule or hold applies, data is preserved according to the default retention rule.
- **What happens when a user deletes a message or file:** The message or file is removed from that user's account. However, when the default retention rule or a custom rule applies, the message or file is still available in Vault for the remainder of the retention period.

[Click here for more on how retention works](#)

Google Workspace for Education Plus

Collaborate easily. Streamline instruction.
Safeguard your learning environment.



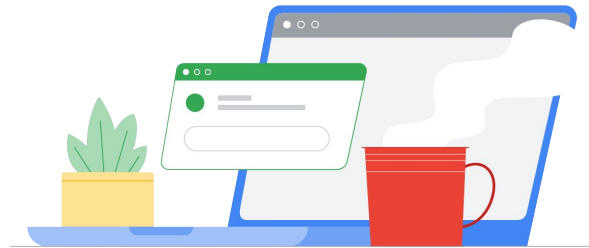
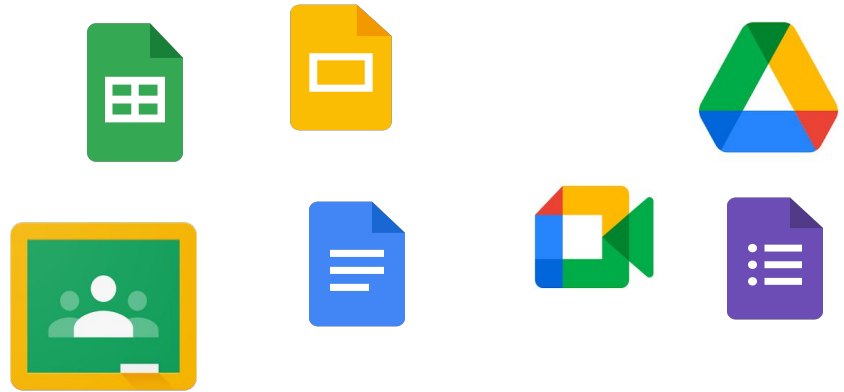
Google for Education

Google Workspace for Education Plus

Have you taken advantage of your FREE* upgrade to
Google Workspace for Education Plus?

[Click here to register your interest](#)

*Google Workspace for Education Plus is free for New Zealand State and State integrated schools



Google Workspace for Education editions offer choice and flexibility

Google Workspace for Education Fundamentals

Provide a **flexible and secure foundation** for teaching and learning with a suite of easy-to-use tools available at no cost.

Google Workspace for Education Standard

Build on all the capabilities of Education Fundamentals with **advanced security and analytics tools** to help reduce risks and mitigate threats with increased visibility and control across your learning environment.

Teaching and Learning Upgrade

Build on all the capabilities of Education Fundamentals or Education Standard and **enhance instructional impact** with tools that make learning more personalized, create classroom efficiency, and enable teaching and learning from anywhere.

Google Workspace for Education Plus

Empower your institution with an **all-in-one EdTech solution**, including all the advanced security, insights, teaching, and learning capabilities from all other Google Workspace for Education editions and features exclusive to Education Plus.

Paid editions

Education Plus provides a proactive approach against security threats with its advanced features



Security dashboard

View instant reports on file exposure, authentication, and settings.



Context-Aware Access

Create policies for who can access apps based on user identity, location, device security status, and IP address.



Alert center

Get real-time security alerts and insights on phishing, malware, and other threats.



Investigation tool

Identify, triage, and take action on security and privacy threats.



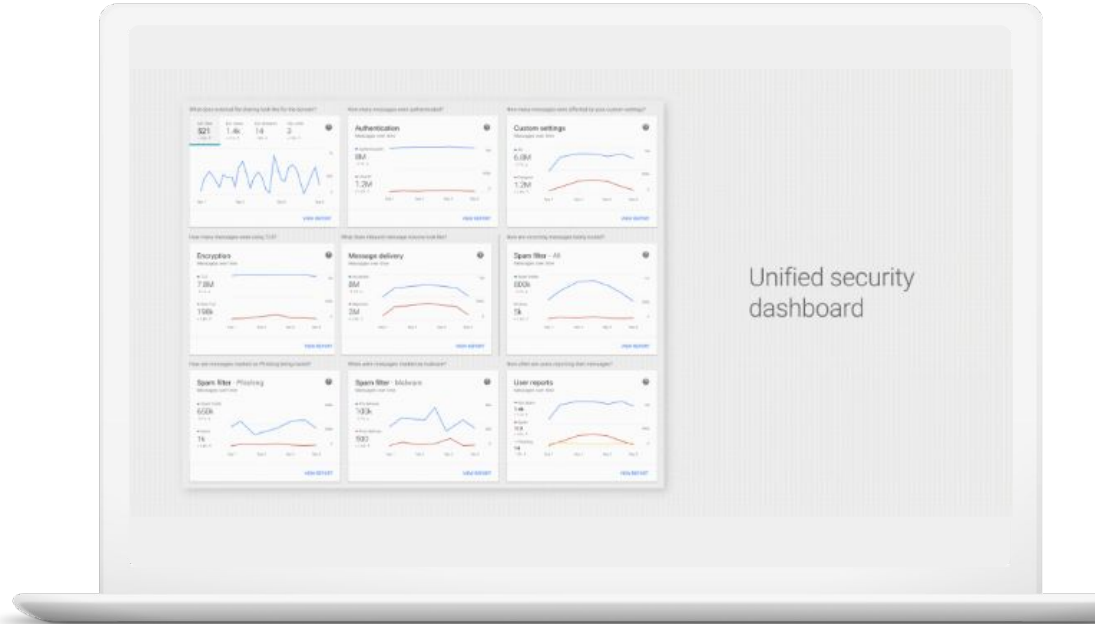
Security sandbox

Automatically scan email attachments to identify potential malware.

Security dashboard

Oversee your domain activity with instant reports on file exposure, authentication, and settings

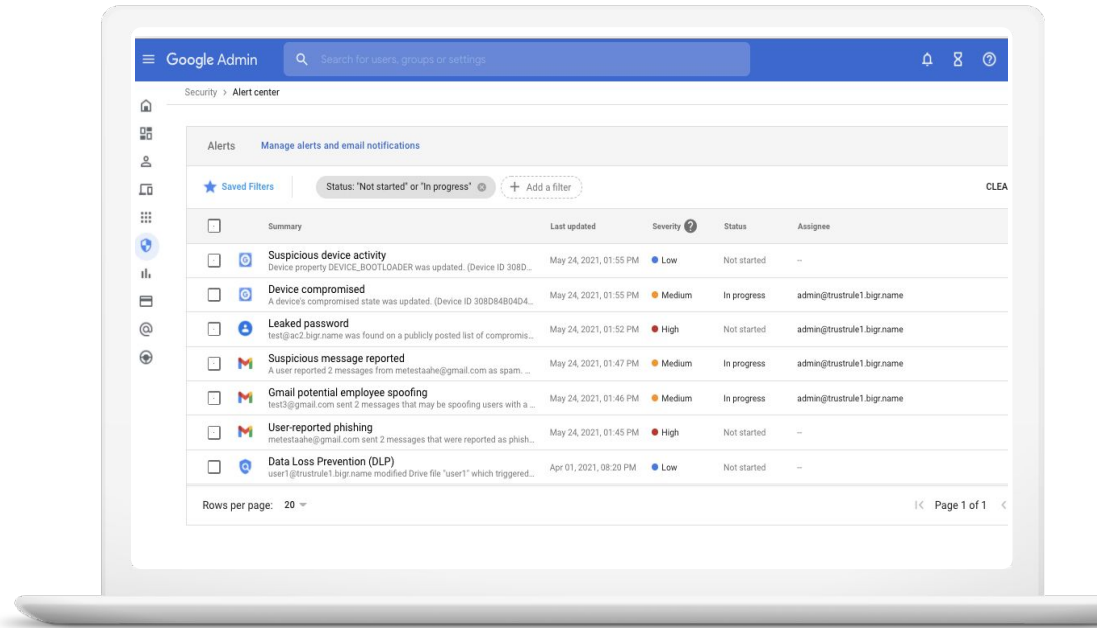
- Streamline cyber threat monitoring and analysis
- Assess your data exposure and risk with more visibility and analytics capabilities
- Improve insights into how your domain's data is being exposed through file sharing
- Gain visibility into phishing messages targeting users within your institution
- Use metrics to demonstrate your security effectiveness



Alert center

View critical security alerts and activity across your domain

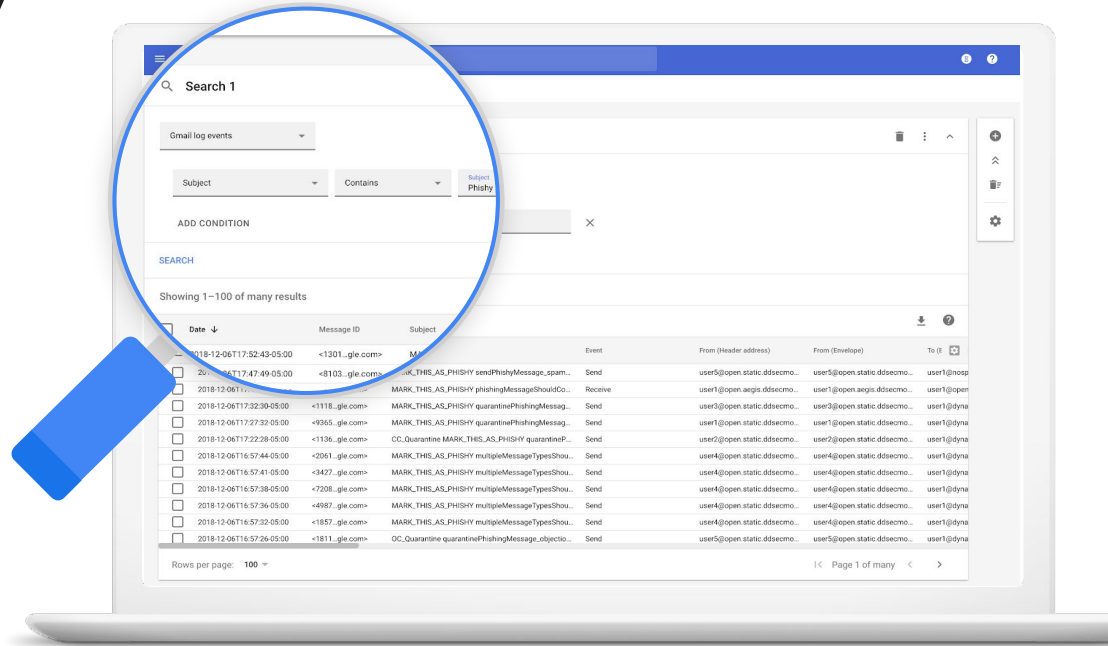
- Access comprehensive alerts across Google Workspace users and apps in the Google Admin console
- Find in-depth alert details that enable you to take action to resolve security issues
- Act in real-time when suspicious activity like phishing, malware, and spam is detected
- View your domain's alert history and add comments to keep a detailed record of any actions you take



Investigation tool

Identify, triage, and take action on security and privacy issues across your domain

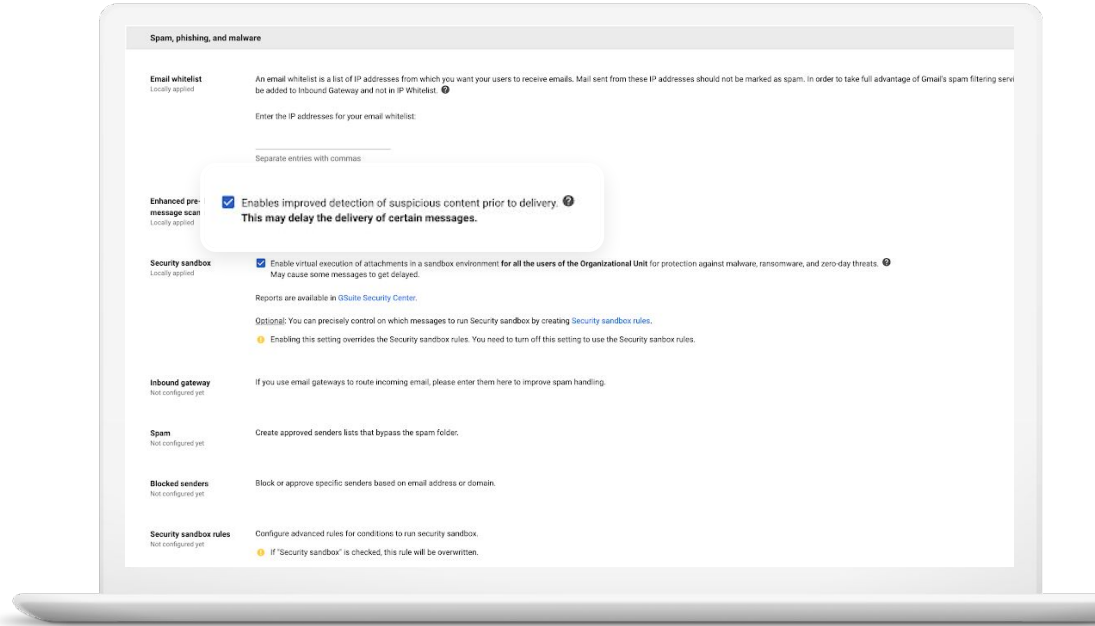
- Target and address phishing, spoofing, and other issues quickly
- Remediate threats with tools that let you quickly explore, triage, and take action
- Identify and prioritize security issues within your domain using deep search capabilities
- End any meeting in your institution right from the investigation tool to help ensure a safer learning environment



Security sandbox

Automatically scan email attachments to identify potential malware

- Set up Gmail to scan all supported attachment types or specify rules for attachment scanning
- Create rules to scan content for specific keywords, account types, domains, and address lists
- Create automations to move risky emails to Spam or quarantine



Education Plus helps enhance instructional impact with flexible, easy-to-use tools



Practice sets

Transform teaching content into interactive assignments with built-in hints.



Originality reports

Compare student work against the web and your school-owned repository.



Interactive questions for YouTube videos

Reinforce concepts with self-paced video lessons in Google Classroom.



Classroom analytics

Gain visibility into student performance and engagement.



Classroom add-ons

Access your favorite third-party tools right within Classroom.



Share class templates and classwork

Simplify lesson planning across your school with shareable curricula in Classroom.



Enhanced Google Meet capabilities

Engage students with breakout rooms, recordings, live captions, and more.



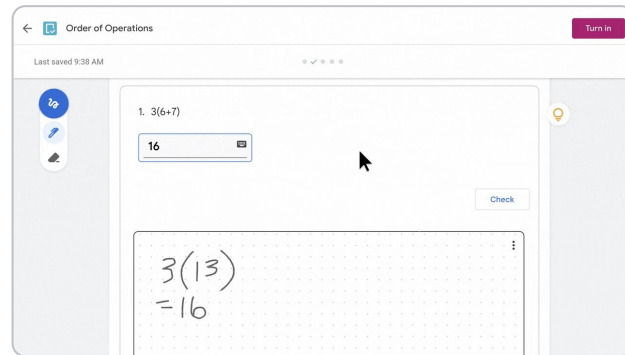
Personalize learning experiences

Engage and guide students at their own pace with practice sets

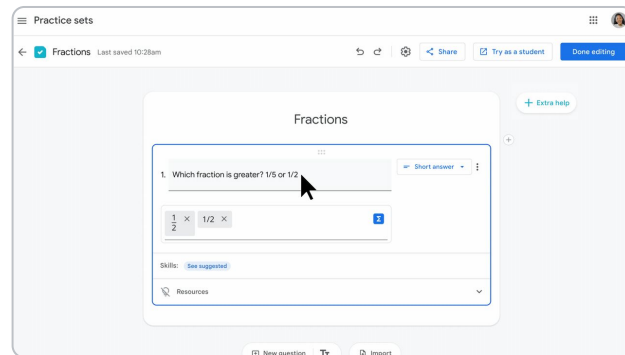
Create interactive assignments to gain valuable insights at both the student and class levels and, with the help of AI, offer hints for students when they get stuck.

- Create new digital lessons from scratch or upload their existing PDF class material
- Provide point-of-use support, with real-time feedback and in-the-moment hints, with the help of AI
- Get insights into student performance
- Share practice sets with other verified teachers in your district

Students get real-time feedback and in-the-moment hints



Teachers can manage the suggested resources and add their own*



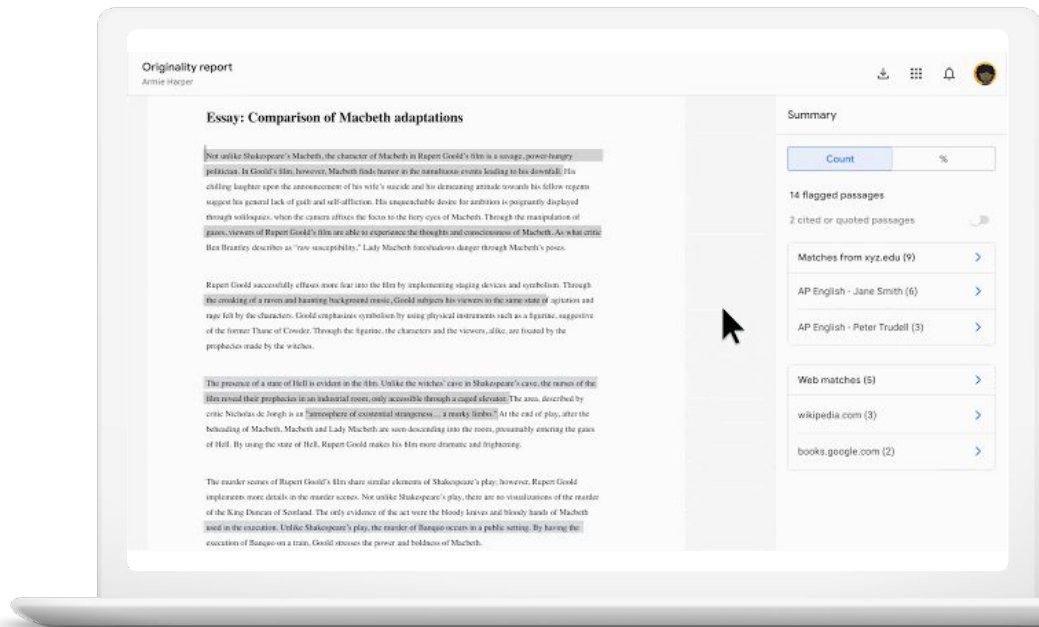


Personalise learning experiences

Encourage critical thinking with originality reports

Help students properly integrate external inspiration into their writing, while making it easy for educators to screen for academic integrity.

- Enable students to check for unintentional plagiarism and recommended citations
- Get unlimited originality reports to compare current student work to anything previously scanned to your private, school-owned repository
- Backfill your repository with past classwork – in addition to hundreds of billions of web pages and over 40 million books
- Keep scanned student work in a secure environment where admins can add or remove files



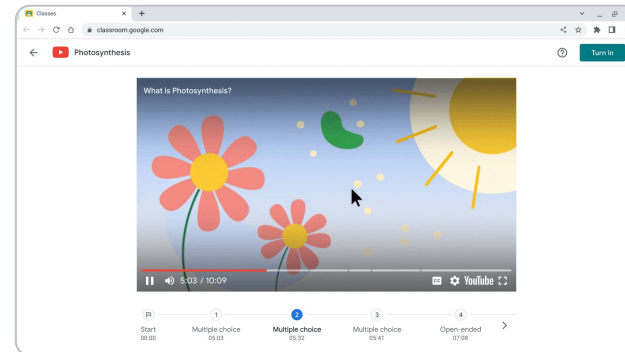


Personalise learning experiences

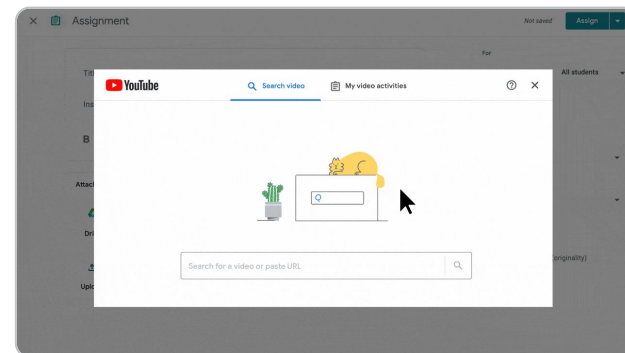
Reinforce concepts with interactive questions for YouTube videos

Save time when creating interactive video activities within Classroom that give students real-time feedback as they watch, and provide insights for teachers.

Students can check their understanding as they watch



Teachers can create their own questions, or select and edit questions that are auto-generated with AI



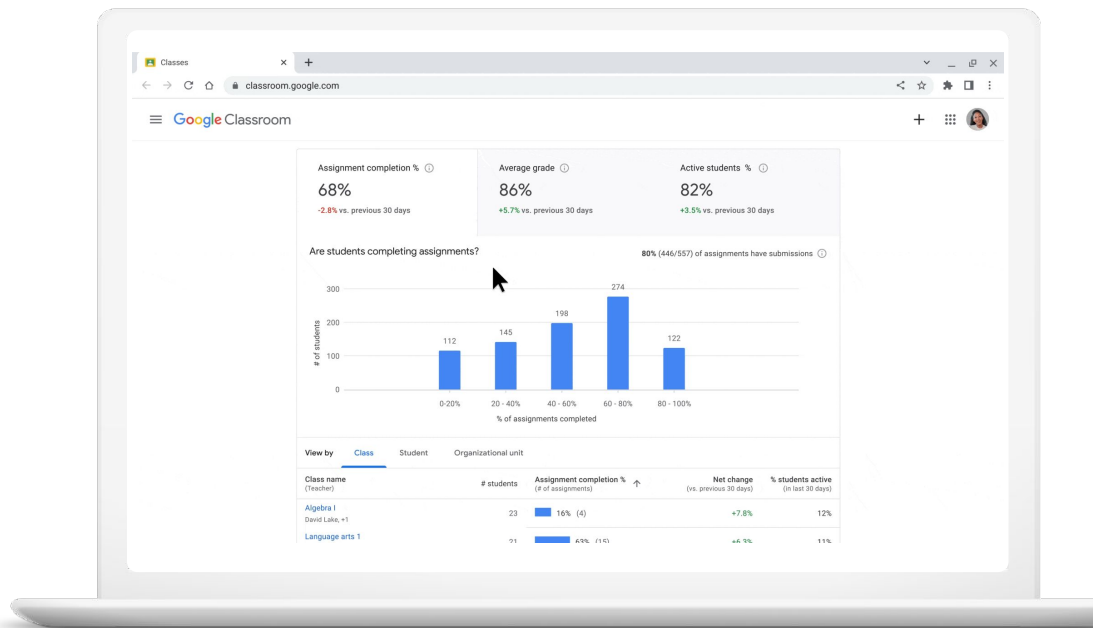


Simplify class management

Make informed decisions with Classroom analytics

Designated education leaders¹ and staff will be able to gain visibility into student performance and engagement, including whether assignments are being completed, how grades are trending, and how Classroom is being adopted. Teachers will be able to view similar information for their own classes, too.

1. Google Workspace admins must [enable](#) Classroom analytics for designated education leaders. Teachers will automatically be able to see class-level analytics for their classes.





Simplify class management

Enhance lessons with Classroom add-ons

Save time and easily find, add, use, and grade content using some of the most popular EdTech tools.

- Access add-ons within Google Classroom using a single sign-on
- Grade and review work directly from add-ons, within Classroom
- Install add-ons across an entire domain with a few clicks – add-ons are available in the Google for Education App Hub

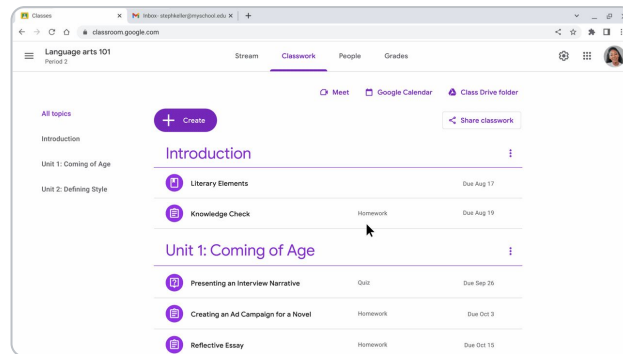
Simplify class management

Simplify lesson planning with shareable class templates and classwork

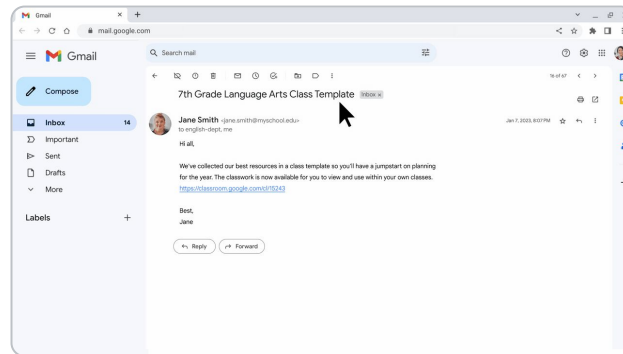
Share links to high-quality classes and class templates, so other educators in your organization can preview and import classwork.

Curriculum

leaders: Start building class templates now before the beta, so your institution is ready when it launches.



Teachers: Preview and import classwork from your peers without having to be a co-teacher.





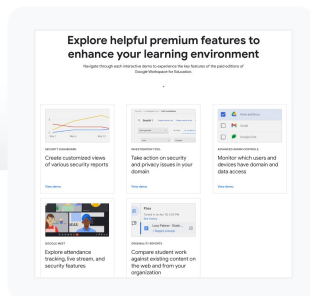
Teach and learn from anywhere

Enhanced Google Meet capabilities

- Engage students with breakout rooms and interactive Q&A and polls
- Connect larger audiences with 1,000 attendees in Meet with 500 contributors and 500 viewers
- Remove language barriers with live translated captions
- Record class and send it out to those who couldn't attend
- Host public livestreams that anyone outside of your school domain can attend
- Review what was shared in class with meeting transcripts
- Make it easier to focus on key participants with tile pairing



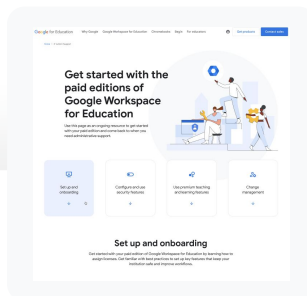
Resources to support your deployment and maximise your investment



Product demos

Demos of Education Plus simulates security and teaching and learning features to help you make an informed decision.

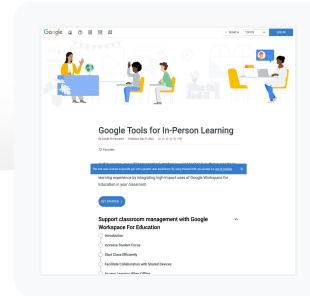
[Tour product demos](#) ↗



IT admin resources

Resource page for IT admins to access onboarding, change management, and ongoing training resources to get started with the premium editions of Google Workspace for Education.

[View IT resources](#) ↗

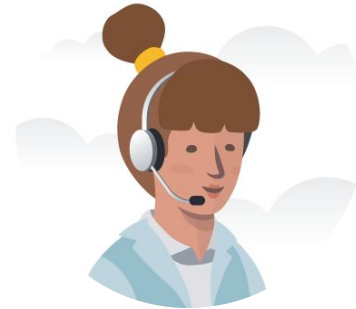


Educator training

This step-by-step training teaches practical strategies for how to use Google tools for in-person learning and classroom management.

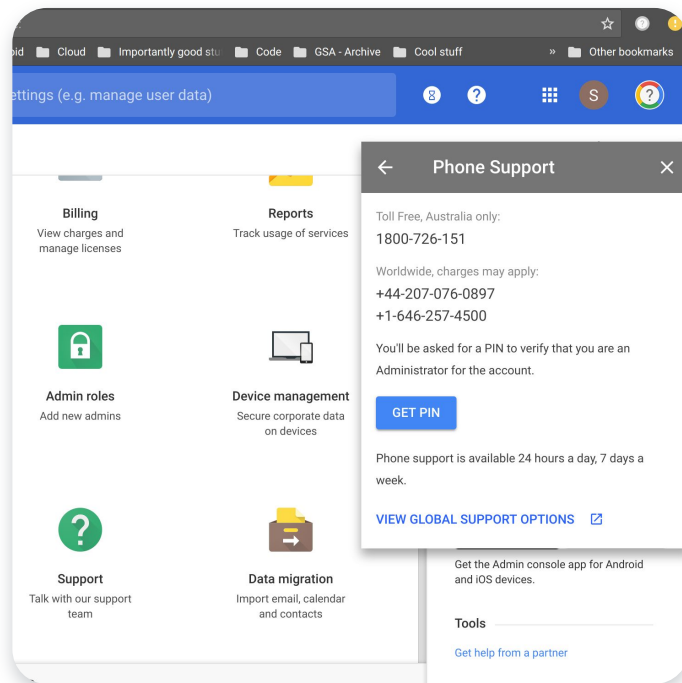
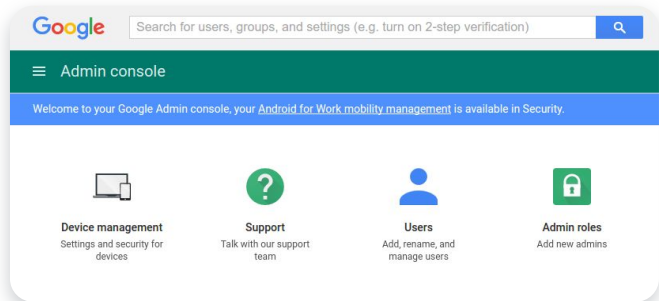
[View training](#) ↗

Support & Troubleshooting



Requesting Support

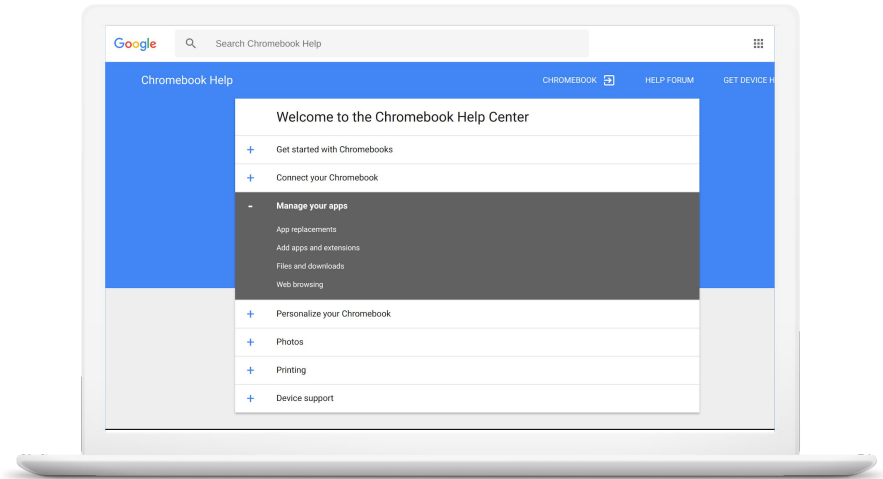
- Enterprise Support PIN in Google Admin Console Support page
- Email and Phone support available 24/7
- Extensive online resources [available here](#)



Chrome Help Centre

<https://support.google.com/chrome>

- Troubleshooting and resolving common issues
- Fix hardware and system problems
- Managing Chrome devices
- [Known Issues](#)
- [Release Blog](#)



Stay Involved as a Chrome Admin

Update feed: alerts you to any changes and additions we make to the product, with updates announced about once a week. Subscribe [here](#).

Email subscription: you can get the update feed info sent to you in an email message (up to one message per day). Subscribe [here](#).

Blogs: the following official Google blogs provide useful and timely information about Google Apps:

- [Google Enterprise Blog](#): Updates and stories about all Google Enterprise products, including Chrome for Business
- [Google Chrome Blog](#): For the latest news about the Chrome browser and Chrome Devices
- [Google Chrome Releases Blog](#): Release notes and feature announcements