

Google Workspace Security

K-12 hardening playbook

Jim Tyler, Director of Technology, Niles Community Schools · MAEDS 2026

A plain-language guide to locking down a K-12 Google Workspace for Education tenant: district devices only, United States only, maximum data protection, and student misuse controls, with separate rules for staff and students.

Every item answers three questions: **What** to set, **Why** it matters, and **Where** it lives in the Admin console (admin.google.com unless noted). Rows are meant to be scanned during a presentation or used as a working checklist.

CONTENTS

- | | |
|---|--|
| 1. License legend | 9. Phase 3c: Turning off AI for student OUs |
| 2. Before you start | 10. Appendix: Additional Google services checklist for the Students OU |
| 3. Phase 0: Identity basics | 11. Phase 3d: Seams the review surfaced |
| 4. Phase 1: Make devices identifiable | 12. Phase 4: Keep it that way |
| 5. Phase 2: Context-Aware Access (CAA) | 13. What you can do today, before any upgrade |
| 6. Phase 3: Data protection | 14. Rollout order |
| 7. Phase 3a: Domain-wide delegation and service-account hygiene | 15. Staff vs. Students at a glance |
| 8. Phase 3b: Student misuse controls | 16. Mac login tools (Mosyle Auth, Jamf Connect, similar) |

License legend

TAG	MEANING
FREE	Available on Education Fundamentals (or any edition). Do these first, before any upgrade lands.
PAID	Requires Google Workspace for Education Standard or Plus (Context-Aware Access, DLP, Security Center, advanced endpoint management). Licensed per user.
ADD-ON	A separate purchase on top of Education Plus (Chrome Enterprise Premium, Gemini Enterprise, Google Voice). Listed so nobody budgets for it by accident.
CEU	Requires Chrome Enterprise Upgrade on the Chromebook. Licensed per device, sold with the hardware, never on a Workspace quote. If a Chromebook shows as Provisioned in Devices > Chrome > Devices, it has CEU.

Quick rule: everything in Phase 2 and the DLP rows in Phase 3 are PAID. Nearly everything else is FREE or CEU.

Licensing trap: PAID features only enforce on users who hold the license. Education Standard/Plus is licensed by total student count and covers all users. A staff-only purchase leaves student OUs unprotected. Renewals require a student enrollment verification letter; keep the student license count at or above enrollment.

Before you start

☐ Confirm the edition covers every user, students included

WHY	See licensing trap above.
WHERE	Billing > Subscriptions
LICENSE	N/A

☐ Split OUs: Staff and Students

SET TO	Split OUs: Staff and Students (K-2, 3-5, 6-8, 9-12), plus Chromebook device OUs by building or cart
WHY	Every policy below is applied per OU. Students and staff need different rules.
WHERE	Directory > Organizational units
LICENSE	FREE

☐ Create a break-glass super admin

SET TO	Create a break-glass super admin (security key, excluded from all CAA, credentials stored offline)
WHY	A bad CAA rule locks admins out too.
WHERE	Directory > Users, then Account > Admin roles
LICENSE	FREE

☐ Pick a pilot group

SET TO	Pick a pilot group (a few IT staff + one grade band or building)
WHY	Every phase goes to pilot first.
WHERE	Directory > Groups
LICENSE	FREE

Phase 0: Identity basics

☐ Enforce 2-Step Verification for staff

SET TO	Enforce 2-Step Verification for staff : check "Allow users to turn on 2-Step Verification", then Go to advanced settings > Enforcement > Turn on enforcement now > "Select allowed 2-step verification methods" = Only security key
WHY	Stolen passwords are the #1 way accounts get taken over. Keys can't be phished. Passkeys count as security keys unless the Passkeys Restriction card limits them to hardware keys. Track enrollment first at Reporting > User reports > Security; enforcing before enrollment locks people out.
WHERE	Security > Authentication > 2-step verification
LICENSE	FREE

☐ Do not enforce 2SV on students

WHY	Students can't reliably hold a second factor. Device-only access (Phase 2) is their second factor.
WHERE	Same screen, scoped to Students OU
LICENSE	FREE

☐ Google session length 12 to 24 hours (staff)

SET TO	Google session length 12 to 24 hours (staff); Google default is 14 days
WHY	Limits how long a stolen session cookie works. Shorter causes re-prompts on Mac login tools. Users must sign out and back in before a new length applies. Admin console sessions are fixed at 1 hour regardless.
WHERE	Security > Access and data control > Google session control
LICENSE	FREE

☐ Mark student OUs as under 18

WHY	Auto-restricts YouTube, Gemini, and other 18+ services. Does not turn off Sites, Groups, Blogger, or Remote Desktop; those still need explicit Off in Phase 3.
WHERE	Account > Account settings > Age-based access settings
LICENSE	FREE

☐ Mark Staff OU as 18 or older

WHY	K-12 organization types often default the root to under-18, which silently strips Gemini and YouTube from teachers.
-----	---

WHERE	Same screen, scoped to Staff OU
-------	---------------------------------

LICENSE	FREE
---------	-------------

☐ Login challenges: employee ID for staff

SET TO	Login challenges: enable employee ID challenge for Staff (only if the Employee ID field is populated and not on badges); leave off for Students unless the ID is something classmates don't know
--------	---

WHY	Challenges are always on; this only adds employee ID to the list Google can ask for. Student IDs are on lunch cards and rosters, so they add nothing.
-----	---

WHERE	Security › Authentication › Login challenges
-------	--

LICENSE	FREE
---------	-------------

Phase 1: Make devices identifiable

CAA can't enforce "district devices only" until Google knows which devices are the district's.

Staff (Windows / Mac)

☐ Confirm Endpoint Verification is on (it is on by default)

SET TO	Confirm Endpoint Verification is on (it is on by default): "Collect device signals using endpoint verification" checked
WHY	This is how Google sees a laptop's encryption, screen lock, and OS version. Supported on Windows 10/11, macOS, ChromeOS 110+, Linux; requires Chrome.
WHERE	Devices > Mobile & endpoints > Settings > Universal > Data access > Device signals
LICENSE	FREE to install; PAID to use in CAA

☐ Force-install the Endpoint Verification extension for the Staff OU

SET TO	Force-install the Endpoint Verification extension for the Staff OU; push Chrome itself via MDM (Macs) or Chrome Browser Cloud Management (Windows)
WHY	EV must be present before the user's first login or CAA denies them.
WHERE	Devices > Chrome > Apps & extensions > Users & browsers > Add from Chrome Web Store > Endpoint Verification > Force install
LICENSE	FREE

☐ Turn on Device approvals for laptops

SET TO	Turn on Device approvals ("Require admin approval"), notification email to an IT group, then approve district laptops in the approvals list
WHY	"Approved" is the cleanest "ours vs. not ours" signal. Blocking an EV device does not stop it syncing on its own; the CAA level must require approved status, which is why Phase 2 checks "admin-approved." Company-owned devices registered by serial number are auto-approved.
WHERE	Devices > Mobile & endpoints > Settings > Universal > Security > Device approvals; then Devices > Mobile & endpoints > Device approvals
LICENSE	FREE

Staff phones (personal)

☐ Mobile management: Basic for staff

SET TO	Mobile management = Basic for Staff OU
WHY	No profile or app on personal phones. Google enforces screen lock and can sign the account out remotely, and CAA can use basic-managed status, OS version, and encryption (those two can take days to sync after enrollment).
WHERE	Devices > Mobile & endpoints > Settings > Universal > General > Mobile management
LICENSE	FREE

☐ Device approvals for phones

SET TO	Device approvals for phones: not available under Basic management (Android and iOS approvals require Advanced management). Choose: Basic + a CAA "managed device" condition (no per-phone approval), or Advanced with a work profile for approvals
WHY	Google's requirement, not a setting. Basic management still lets CAA block unmanaged phones, which is the outcome that matters; you just won't get a Pending/Approve queue for personal phones.
WHERE	Devices > Mobile & endpoints > Settings > Universal > Security > Device approvals (Advanced only)
LICENSE	FREE

☐ Auto-wipe account after 30 days inactive or reported lost

WHY	Old phones stop carrying district mail.
WHERE	Same Universal settings > Security
LICENSE	FREE

☐ Advanced mobile management for district-owned phones only

SET TO	Advanced mobile management for district-owned phones only (optional)
WHY	Adds encryption, OS version, and compromised-device checks to CAA.
WHERE	Same > Mobile management, scoped to a district-phone OU
LICENSE	PAID

Students (Chromebooks)

☐ Every student Chromebook enrolled in the right device OU

WHY	Enrolled ChromeOS passes CAA device checks natively, no EV needed.
-----	--

WHERE	Devices > Chrome > Devices
-------	----------------------------

LICENSE	CEU
---------	------------

☐ Forced re-enrollment

SET TO	Forced re-enrollment = "Force device to automatically re-enroll after wiping" (this also disables developer mode); Powerwash = "Do not allow"; Verified access on; Guest mode = Disable (K-12 default)
--------	--

WHY	Prevents un-enrolling or wiping the device to escape policy. There is no separate developer-mode switch; forced re-enrollment is it.
-----	--

WHERE	Devices > Chrome > Settings > Device settings > Enrollment and access; Sign-in settings
-------	---

LICENSE	CEU
---------	------------

☐ Block sign-in from non-district accounts

WHY	Keeps personal Gmail off district hardware.
-----	---

WHERE	Devices > Chrome > Settings > Device > Sign-in restriction
-------	--

LICENSE	CEU
---------	------------

☐ Push web filter extension

WHY	CIPA and basic safety.
-----	------------------------

WHERE	Devices > Chrome > Apps & extensions
-------	--------------------------------------

LICENSE	CEU
---------	------------

☐ Readiness check before CAA

SET TO	Readiness check before CAA: clear "OS version not compliant" and "Policies can't be applied" tiles; push pending updates; retire devices past Auto Update Expiration
WHY	Those devices fail minimum-OS and verified-boot conditions the day CAA is enforced.
WHERE	Devices > Chrome > Devices (notification tiles at top; View upgrades for license count)
LICENSE	CEU

Gate: inventory is clean, every device that should pass is enrolled and approved, departed users' devices removed.

Phase 2: Context-Aware Access (CAA)

Everything in this phase is PAID. All CAA work lives at **Security > Access and data control > Context-Aware Access**. Two things first: click **Turn On** on that page (assignments do nothing until CAA is on; turning it off again takes up to 24 hours to fully clear), and have every staff user sign into Endpoint Verification and refresh their browser before any device policy goes active, or they get denied even on a compliant device.

Basic mode is enough for almost everything here. It offers these attributes: IP subnet, Location (countries), Device policy (admin approval required, company-owned required, screen lock, encryption), Device OS with a minimum version (macOS, Windows, Linux, ChromeOS, iOS, Android), and "meets an existing access level." Conditions can be joined with AND/OR, and a condition can be set to "Don't meet attributes" for deny lists. Advanced mode (CEL) is only needed for attributes Basic mode lacks, such as ChromeOS verified boot (`device.verified_chrome_os == true`). Never edit Workspace access levels from the Google Cloud console; it can inject unsupported attributes and block everyone.

Access levels to create

LEVEL	CONDITIONS	WHY
US-Only	Location = United States, optionally OR IP subnet (Public) = district VPN egress range	Almost all attacks on school accounts originate outside the US. Basic mode.
Staff-Device	Device policy: admin approval required + encrypted + screen lock; Device OS: Windows/macOS with minimum version	Stolen credentials are useless without a district laptop. Basic mode. Requires Device approvals on and laptops approved first.
Staff-Mobile	Device policy: screen lock + encrypted; Device OS: iOS/Android with minimum version	Blocks unmanaged phones, because an unmanaged phone reports none of these attributes. Basic mode. Do not add "admin approval required" unless the OU is on Advanced management; basic-managed phones can never be approved. Encryption and OS version can take days to sync after enrollment.
Student-Device	Device OS = ChromeOS with minimum version, plus company-owned required; add verified boot in Advanced mode (<code>device.verified_chrome_os == true</code>)	Students can only reach Google from a district Chromebook. Enrolled Chromebooks are company-owned automatically. Verified boot is CEL-only.
Student-Mac (only if Mac labs use a Google-backed login tool)	Same as Staff-Device, scoped to lab OU	Lab Macs would otherwise be blocked.
Staff-Travel	Same device conditions as Staff-Device, AND a second condition set to "Don't meet attributes" with Location = high-risk deny list	Travelers keep working; device requirement never drops. Basic mode handles the deny list.

Assignments

WHAT	WHY	WHERE
Combine US-Only AND the device level; assign to Gmail, Drive/Docs, Calendar, Meet, Chat, Keep, Sites, Tasks, Cloud Search, Vault, Gemini, Gemini Notebook, Workspace Studio, and the Admin console	Both conditions must be true. Assigning multiple levels to one app is an AND. Assign light apps first, Gmail last, per Google's rollout guidance.	Context-Aware Access > Assign access levels
Assign by group for travel, by OU for everything else	Group assignments override OU without moving the user.	Same
Apply only US-Only (never a device level) to any Mac login tool's OAuth app (Mosyle Auth, Jamf Connect, etc.), or exempt it entirely	A fresh Mac has no EV yet; a device rule would block first login. Google documents both assigning levels to third-party apps and exempting trusted ones.	Context-Aware Access > Assign access levels > Third-party apps
Monitor mode first, at least one week, pilot OU	See who would be denied before anyone actually is. Denials that would have happened appear in Context-Aware Access log events.	Each assignment > Monitor; Reporting > Audit and investigation > Context-Aware Access log events

Known limits (tell the help desk)

- Geolocation is IP-based. Some carriers and home ISPs misplace users occasionally.
- Native mobile apps on an unapproved phone fail silently, no error.
- Third-party SAML/OAuth apps are only covered if you assign CAA to them explicitly.

Travel exception workflow

1. Staff submits travel dates and countries (form/ticket).
2. IT adds them to a **travel-exception** group, which carries **Staff-Travel**.
3. Auto-remove on return date (group membership expiration, or a short Apps Script).
4. Admins traveling use the break-glass procedure, not the travel group.
5. Loaner Chromebook for high-risk destinations; wipe on return.
6. No student travel exception. Student Chromebooks are simply blocked abroad.

Gate: zero unexpected denials in the CAA log during monitor week; break-glass tested; Mac login verified with 2SV on a freshly enrolled Mac; help desk briefed. If something goes wrong after activation, delete the offending access level rather than turning CAA off: deleted levels stop applying immediately, while Turn Off can take 24 hours.

Phase 3: Data protection

Both lanes

☐ DLP rules with predefined detectors

SET TO	DLP rules with predefined detectors (SSN, credit card, birthdate, address, credentials) on Drive and Chat
WHY	Catches PII leaving the district automatically.
WHERE	Security › Access and data control › Data protection
LICENSE	PAID

☐ Add CAA conditions to DLP rules

SET TO	Add CAA conditions to DLP rules (block download/print/copy off approved devices)
WHY	Closes the gap where a viewer on a personal machine could still export.
WHERE	Same › Rule › Conditions
LICENSE	PAID

☐ Classification labels for Drive

SET TO	Classification labels for Drive; use as DLP conditions, or let DLP apply them automatically
WHY	Lets DLP target "Student Records" instead of scanning everything.
WHERE	Security › Access and data control › Classification labels (Label Manager); Apps › Drive and Docs › Labels to turn them on for users
LICENSE	PAID

☐ Chrome DLP

SET TO	Chrome DLP (upload/download/paste) on managed browsers
WHY	Catches data leaving through the browser itself. Google: "features are available only for customers who have purchased Chrome Enterprise Premium." Skip unless budgeted.
WHERE	Security › Access and data control › Data protection (Chrome trigger) + Chrome Enterprise connector policies
LICENSE	ADD-ON (Chrome Enterprise Premium, not included in Education Plus)

☐ Google Takeout

SET TO	Google Takeout: shared control Not allowed (K-12 default), plus the individual per-service controls (YouTube and others default to Allowed) set to Not allowed for students; "Transfer your content" unchecked except for a graduating-seniors OU in spring
WHY	Stops one-click export of an entire account. K-12 domains already have the shared control off, but the per-service Takeout controls default to Allowed and the graduating-student transfer tool is a separate checkbox on the same page.
WHERE	Data > Data import & export > Google Takeout > User access to Takeout for Google services; Additional transfer permissions
LICENSE	FREE

☐ Block unconfigured third-party apps

SET TO	Block unconfigured third-party apps; allowlist vetted apps only
WHY	Rogue OAuth apps are a common data-theft path. Note: users labeled under 18 are already blocked from unconfigured apps by Google; the only choice for them is whether to allow apps that request basic Sign in with Google info only. Students then "request access," and requests show on the Admin console home App access control card.
WHERE	Security > Access and data control > API controls
LICENSE	FREE

☐ Mark MDM and Mac login OAuth clients as Trusted BEFORE flipping the block

WHY	Otherwise Mac logins and user sync stop.
WHERE	Same > Manage third-party app access
LICENSE	FREE

☐ Restrict Marketplace installs

WHY	Same reason as above.
WHERE	Apps > Google Workspace Marketplace apps > Settings
LICENSE	FREE

☐ Gmail: no external auto-forwarding, no POP/IMAP

SET TO	Gmail: disable auto-forwarding to external, disable POP/IMAP
WHY	Forwarding rules are the classic silent exfiltration.
WHERE	Apps > Google Workspace > Gmail > End user access
LICENSE	FREE

☐ Gmail: enhanced scanning and external recipient warning

SET TO	Gmail: enhanced pre-delivery scanning, external recipient warning
WHY	Phishing and "oops, wrong recipient."
WHERE	Apps > Google Workspace > Gmail > Safety
LICENSE	FREE

☐ Gmail: attachment compliance

SET TO	Gmail: attachment compliance (see recipe below)
WHY	Password-protected zips and disk images are how malware gets delivered; Google can't scan inside them. Google already rejects executables automatically.
WHERE	Apps > Google Workspace > Gmail > Compliance > Attachment compliance
LICENSE	FREE

☐ Gmail: content compliance for SSNs and card numbers

SET TO	Gmail: content compliance with predefined matchers (SSN, credit card) on outbound, Medium confidence, min match 1
WHY	PII in the body or attachments. Belt to DLP's suspenders. Predefined matchers save but do nothing on Fundamentals.
WHERE	Apps > Google Workspace > Gmail > Compliance > Content compliance
LICENSE	PAID

☐ Gmail: regex fallback for SSNs

SET TO	Gmail: regex fallback for formatted SSNs (<code>\b\d{3}-\d{2}-\d{4}\b</code>) on outbound
WHY	Works with no license dependency; noisier than predefined matchers.
WHERE	Same > Advanced content match > Body > Matches regex
LICENSE	FREE

❑ Turn OFF Chrome Remote Desktop

SET TO	Turn OFF Chrome Remote Desktop (service) for all OUs
WHY	Lets anyone with the account remote-control a district device from anywhere, bypassing every device and location check.
WHERE	Apps > Additional Google services > Chrome Remote Desktop
LICENSE	FREE

❑ Remote access on ChromeOS

SET TO	Remote access on ChromeOS: Remote support connections = Prevent remote support connections ; Remote access hosts and Remote access clients = district domains (one per line); Firewall traversal = Disable ; leave Enterprise remote support connections allowed so IT can still connect from the Admin console
WHY	Students can't start or accept a Chrome Remote Desktop session; personal accounts can't be on either end; IT's Admin-console remote support keeps working.
WHERE	Users & browsers > Remote access
LICENSE	FREE (CEU on Chromebooks)

Recipe: Gmail attachment compliance rule

Path: Apps > Google Workspace > Gmail > Compliance > Attachment compliance > Add setting

FIELD	VALUE	WHY
Description	Quarantine encrypted and risky inbound attachments	Required field.
Email messages to affect	Inbound only	Quarantining outbound holds staff mail silently. Never quarantine outbound; use a separate Reject rule if needed.
Expressions (If ANY match)	File type > Office documents which are encrypted; Compressed files and archives which are encrypted	Google can't scan inside password-protected files.
Custom file types	iso, img, vhd, vhdx, lnk, hta, js, jse, vbs, vbe, wsf, wsh, ps1, scr, bat, cmd, reg, msi, jar	Runs when double-clicked but slips past the built-in executable filter. Disk images and .lnk shortcuts are current top phishing payloads.
Also match files based on file format	Checked	Catches renamed files.
Leave unchecked	Unencrypted Office docs, unencrypted archives, images, video, audio	Normal school traffic.
Action	Change Modify message to Quarantine message > Default quarantine	Lets IT release the legitimate ones.
Notify recipient	On for staff, off for students (split the rule per OU if you want both)	Staff can ask IT to release; students shouldn't.
After saving	Watch Apps > Gmail > Manage quarantines for the first week	Adjust the extension list if something legitimate keeps landing there.

Optional stricter student rule: same expressions plus *Compressed files which are not encrypted*, action **Reject**, scoped to Students OU. Students have no reason to receive zips from outside.

Recipe: auditing shared drives and public files

Shared drives outlive the people who made them, and their sharing settings are set per drive by whoever created it. A shared drive created in 2019 with "anyone with the link" enabled is still that way today.

Tenant-wide defaults (set once)

Path: Apps > Google Workspace > Drive and Docs > Sharing settings, then the Shared drive creation section

SETTING	VALUE	WHY
"Prevent users in [OU] from creating new shared drives"	Unchecked for Staff, checked for Students	Student-created shared drives are unmonitored group spaces.
Prevent members from sharing files outside the organization	Checked for Students; checked for Staff unless a specific drive needs external partners	Stops external sharing from a shared drive even if the user's own setting would allow it.
Prevent people who aren't shared drive members from accessing files	Checked	Blocks "anyone in the organization with the link" from reaching shared drive files they weren't given.
Prevent commenters and viewers from downloading, copying, and printing	Checked for Students; optional for Staff	Same control DLP applies, without the license.
Prevent content managers from changing shared drive settings	Checked	Only managers (and admins) can loosen the drive.

New drives inherit these; existing drives keep whatever they had, which is why the audit below matters.

Keep admins' daily-driver accounts out of sensitive drives. The account you read email and browse with all day is the one most likely to be phished, and anything it can open is what an attacker can download with a single stolen session. Put student records, HR, finance, and security documentation in shared drives whose members are a separate admin or role account per person, used only for that work, with no mail delivered to it. Your everyday account should not be a member at all. This cuts both exfiltration risk (the session an attacker is most likely to get can't reach the files) and attack surface (there is no "I'll just open it from my main account" path to misconfigure). The same split applies to super admin: the super admin role should live on an account nobody uses for daily work.

Per-drive audit (quarterly)

☐ List every shared drive and its sharing settings

SET TO	List every shared drive with member count, external members, and its four sharing settings; sort by external members and by "anyone with link" allowed
WHERE	Apps > Google Workspace > Drive and Docs > Manage shared drives (filter: has external members; no members; created by a suspended user)
LICENSE	FREE

☐ Fix drives with no active manager (creator left the district)

SET TO	Fix drives with no active manager (creator left the district): add an IT manager, then reassign
WHERE	Same page > drive > Manage members
LICENSE	FREE

☐ Restrict drives that still allow external or non-member access

SET TO	Restrict settings on any drive that still allows external sharing or non-member access unless it has a documented reason
WHERE	Same page > drive > Settings
LICENSE	FREE

☐ GAM export for a spreadsheet you can keep

SET TO	GAM export for a spreadsheet you can keep: <code>gam print shareddrives fields id,name,createdtime,restrictions</code> and <code>gam print shareddrives ... showmembers</code> ; diff against last quarter
WHERE	GAM
LICENSE	FREE

☐ Find publicly shared files anywhere in the domain

SET TO	Find publicly shared files anywhere in the domain: <code>gam all users print filelist query "visibility='anyoneWithLink' or visibility='anyoneCanFind'" fields id,name,owners,permissions</code> (add <code>select shareddriveid <id></code> for a single shared drive)
WHERE	GAM
LICENSE	FREE

☐ Same search, live, in Drive log events

SET TO	Same search, live and filterable: Drive log events, filter Visibility = Public on the web or Anyone with the link
WHERE	Reporting > Audit and investigation > Drive log events
LICENSE	FREE to view

☐ Bulk-remove public links from the investigation tool

SET TO	Bulk-remove public links straight from the search results, and save the search as an alert rule
WHERE	Security > Security center > Investigation tool > Drive log events
LICENSE	PAID

☐ Dashboard of external file exposure trends

WHERE	Security > Security center > Dashboard > File exposure
LICENSE	PAID

☐ Alert rule: student external shares and public files

SET TO	Alert rule: new externally shared file from a student, or any file set to Public on the web
WHERE	Security > Alert center > Rules
LICENSE	PAID

Remediation

Bulk-remove public and external permissions with GAM rather than by hand: `gam user <owner> delete drivefileacl <fileid> anyone` for a single file, or drive the same command from the export above. Announce before running it; teachers use "anyone with the link" for parent newsletters and will need a trusted-domain or specific-person share instead.

Recipe: detecting malicious mailbox filters

No admin setting prevents users from creating Gmail filters. Attackers use them to auto-archive password resets and invoices so a compromised account stays quiet.

☐ External auto-forwarding off, delegation restricted, third-party OAuth blocked

WHY	Removes the forward-to-attacker action and the API path for silent filter creation.
WHERE	Covered in Phase 3 rows above
LICENSE	FREE

☐ Weekly GAM dump

SET TO	Weekly GAM dump: <code>gam all users print filters</code> , <code>print forwards</code> , <code>print delegates</code> ; diff against last week
WHY	Most reliable detection. Flag delete/archive/mark-read/forward actions paired with terms like <code>password</code> , <code>verify</code> , <code>invoice</code> , <code>wire</code> , <code>payroll</code> , <code>direct deposit</code> .
WHERE	GAM, scheduled
LICENSE	FREE

☐ Read Gmail log events for user settings changes

SET TO	Read Gmail log events for user settings changes (filter, forwarding, delegation)
WHY	Same data as the paid tool, no alerting. Entries appear within about an hour.
WHERE	Reporting > Audit and investigation > Gmail log events
LICENSE	FREE

☐ Alert in real time on risky filter creation

SET TO	Saved investigation-tool search on the same events, turned into an activity rule that alerts on filter creation with a forward or delete action
WHY	Real-time instead of weekly.
WHERE	Security > Security center > Investigation tool > Gmail log events > Create activity rule
LICENSE	PAID

☐ Built-in alerts: suspicious login, forwarding out of domain

SET TO	Built-in alerts: suspicious login, email forwarding out of domain
WHY	Catches the takeover that precedes the filter.
WHERE	Security > Alert center
LICENSE	FREE

☐ Remediate a compromised mailbox

SET TO	Remediate: <code>gam user X delete filter <id></code> , password reset, <code>gam user X deprovision</code> (revokes tokens and sessions), recheck forwards and delegates
WHY	Filter removal alone leaves the attacker's session alive.
WHERE	GAM
LICENSE	FREE

Staff

☐ Drive external sharing: trusted domains only

SET TO	Drive external sharing = allowlisted (trusted) domains only; no "anyone with link"
WHY	Prevents accidental public documents. For finer control (this OU can share with these domains, that OU can't), use Drive trust rules instead of the OU-wide setting.
WHERE	Apps > Google Workspace > Drive and Docs > Sharing settings; Security > Rules > Trust rules for Drive sharing
LICENSE	FREE

☐ DLP action for staff: warn, then block

SET TO	DLP action: warn for 2 weeks, then block
WHY	Lets staff learn before it bites.
WHERE	Data protection > Rule > Actions
LICENSE	PAID

☐ Vault retention rules per district policy

SET TO	Vault retention rules per district policy; holds enabled
WHY	Legal and records requests.
WHERE	vault.google.com > Retention / Matters
LICENSE	FREE (included in Education Fundamentals)

☐ Client-side encryption only when a key service is chosen

WHY	Biggest lift; do last.
WHERE	Security > Access and data control > Client-side encryption
LICENSE	PAID

Students

☐ Drive sharing within domain only

SET TO	Drive sharing within domain only; no link sharing; Drive for desktop off
WHY	Student work stays inside the district.
WHERE	Apps > Google Workspace > Drive and Docs > Sharing settings (Students OU)
LICENSE	FREE

☐ DLP action for students: block

SET TO	DLP action: block external sharing immediately
WHY	Students won't read warnings.
WHERE	Data protection > Rule > Actions
LICENSE	PAID

☐ Gmail internal-only + allowlist of approved external domains

SET TO	Gmail internal-only + allowlist of approved external domains; no delegation
WHY	Stops outside contact and spam.
WHERE	Apps > Google Workspace > Gmail > Compliance > Restrict delivery
LICENSE	FREE

☐ Chat internal-only

SET TO	Chat internal-only; external Meet joins blocked; Meet creation requires staff host (by grade band)
WHY	Same.
WHERE	Apps > Google Workspace > Google Chat > External chat / Google Meet > Meet safety settings
LICENSE	FREE

☐ Turn off services students don't need

SET TO	Turn OFF: Gemini, Play/Marketplace, Sites, Blogger, Groups, Photos, Maps sharing, Chrome Remote Desktop
WHY	Not needed for instruction; each is a data path.
WHERE	Apps > Additional Google services (Students OU)
LICENSE	FREE

☐ Classroom: verified teachers, staff-only classes

SET TO	Classroom: teacher verification on, class creation staff-only, guardian summaries configured
WHY	Prevents fake classes and keeps parents in the loop.
WHERE	Apps > Google Workspace > Classroom
LICENSE	FREE

☐ Classroom API data access ("Users can authorize apps")

SET TO	Classroom API data access ("Users can authorize apps"): leave checked for 3-12 and staff; uncheck only for K-2
WHY	Unchecking breaks student-side integrations (Kami, Edpuzzle, Pear Deck, Nearpod, Classroom add-ons). Restrict which apps can get Classroom scopes in API controls instead: set the Classroom service to Restricted so only Trusted apps qualify.
WHERE	Apps > Google Workspace > Classroom > Data access; Security > Access and data control > API controls > Google services > Classroom
LICENSE	FREE

☐ Vault: separate student retention

SET TO	Vault: separate student retention; suspend at withdrawal, delete after retention window
WHY	FERPA/COPPA and state retention rules.
WHERE	vault.google.com > Retention (Students OU)
LICENSE	FREE

☐ Shorter sessions on shared carts

SET TO	Session: shorter for cart/shared Chromebooks; sign out on lid close
WHY	Next student shouldn't inherit the last one's session.
WHERE	Devices > Chrome > Settings > Device
LICENSE	CEU

Gate: DLP incident reports reviewed; no legitimate workflow blocked; Vault retention documented.

Phase 3a: Domain-wide delegation and service-account hygiene

Domain-wide delegation (DWD) lets a Google Cloud service account act as any user in the tenant without that user's consent or password. It is how backup products, mail-security connectors, directory syncs and in-house scripts read and write every mailbox and Drive. The list of delegated clients is the list of identities that can impersonate your whole organization, and it accumulates for years because nothing expires it and nothing reports on it. Every entry answers four questions: who owns it, what it actually does, whether it is still used, and what happens when the person who created it leaves.

Audit

☐ Inventory the delegation page

SET TO	Export every row — display name, client ID, scope list, and from your own records the owner and purpose. Push entries with no recognizable name, or a name that is a project rather than a product, to the top.
WHY	The page is the only place the names live. Google's audit log records client IDs, not names, so the two have to be joined by hand. No API lists DWD clients.
WHERE	Security > Access and data control > API controls > Manage Domain Wide Delegation
LICENSE	FREE

☐ Match each client to what it actually does

SET TO	For each client ID, pull its token audit events: authorize events give the impersonated users, source IP and requested scopes; activity events give the API and method of every call. Record distinct users, calls per day, source IPs, first and last seen, and top methods.
WHY	Scopes say what a client may do; methods say what it does. A backup reads history and change-list endpoints and never writes; a connector reading every mailbox from a cloud IP range you don't recognize is a different conversation.
WHERE	Reports API, activities.list with applicationName=token, userKey=all, filters="client_id==" (add eventName for methods); 180-day retention
LICENSE	FREE

☐ Remove anything with no activity in the window

SET TO	Zero token events in 180 days means remove the entry. Keep the exported row so it can be re-added in one step if a vendor calls.
WHY	Dormant delegations are standing impersonation rights held by a key you probably can't locate, and nothing visible depends on them. They are the easiest removals in the tenant.
WHERE	Same page > delete; re-add by pasting client ID and scopes
LICENSE	FREE

☐ Name every entry after the product and owner

SET TO	"Backup NAS, building X, owner Y" rather than the name of the Cloud project someone reused. Rename on the page; the client ID doesn't change.
WHY	The next admin has to be able to answer "what is this" from the page alone.
WHERE	Same page > edit
LICENSE	FREE

☐ Minimize scopes to what the methods show

SET TO	Compare the granted scopes with the APIs actually called. Drop write scopes where only reads occur, and unused "nice to have" scopes, unless the vendor's documentation requires them for discovery.
WHY	A read-only backup that holds a user-write scope becomes an account-creation tool the day its key leaks.
WHERE	Same page > edit scopes; test the product afterward
LICENSE	FREE

☐ Separate DWD from per-user OAuth apps

SET TO	Integrations users consent to individually (copier scan-to-Drive, classroom tools, PDF editors) live under App access control, not here. Audit them with the same token-log method, filtered by app name.
WHY	They don't impersonate the whole domain, but a Drive-write app used by 400 people is still a mass-exfiltration path if the vendor is breached.
WHERE	Security > Access and data control > API controls > Manage third-party app access
LICENSE	FREE

Ownership: keep projects, service accounts and keys away from daily drivers

☐ Service-account projects are organization-owned

SET TO	Every service account that holds a delegation sits in a Cloud project inside your Workspace organization, in a folder reserved for infrastructure. Project Owner and Editor are held by dedicated admin identities only — no personal Gmail, no vendor account, no former employee.
WHY	Whoever owns the project can mint a new key that reads every mailbox the delegation covers. A project created under someone's daily account is orphaned the day they leave and keeps working for anyone who still has that account.
WHERE	console.cloud.google.com > IAM & Admin > IAM; organization folder structure
LICENSE	FREE

☐ One key per consumer, with an expiry

SET TO	Each product or script gets its own service account and exactly one key. Set the org policy iam.serviceAccountKeyExpiryHours so keys must be re-issued on a schedule (a year suits an appliance). Delete keys you can't name a consumer for.
WHY	A shared key can't be rotated without an outage somewhere, so it never is. A no-expiry key downloaded to a laptop in 2019 is still valid.
WHERE	console.cloud.google.com > IAM & Admin > Service Accounts > Keys; Organization policies
LICENSE	FREE

☐ Keys never touch a daily-driver machine or account

SET TO	Download a key directly on the host that will use it (the appliance, the automation server) or into a secrets store — never into a Downloads folder, a mailbox, a chat, or a daily account's Drive. On servers, the key file's ACL names the one identity that reads it.
WHY	The JSON key is the credential. The usual leak is a copy left where every local user, a backup job, or a transcript can read it — not a breach of the Cloud project.
WHERE	Host file-system ACLs; secrets manager
LICENSE	FREE

☐ Vendor connectors run as a service identity, not a person

SET TO	When a vendor product wants an admin account for its Google connector (mail security, SSO provisioning, archiving), create a dedicated identity with exactly the admin role it needs. Never a named admin, never the break-glass.
WHY	The connector keeps running as that person after they change roles or leave, and its thousands of daily calls appear in the log under their name, hiding any real activity by that account.
WHERE	The vendor's admin portal; Directory > Users; Account > Admin roles
LICENSE	FREE

❑ Google auto-provisioning runs as whoever enabled it

SET TO	SAML app auto-provisioning is authorized under the admin who set it up and re-binds to whoever re-authorizes it. Authorize it from a dedicated provisioning admin, and re-authorize from that identity after admin turnover.
WHY	It generates a steady stream of token events under that admin forever. If that was the break-glass account, the account that should be silent is the noisiest in the log.
WHERE	Apps > Web and mobile apps > (app) > Auto-provisioning
LICENSE	FREE

❑ Break-glass accounts are silent and alerted on

SET TO	No delegation, no provisioning job, no connector bound to the break-glass identity. An alert rule on any login or token event for it.
WHY	The account's value is that any activity on it is an incident. A standing job under it removes that property.
WHERE	Security > Alert center > Rules; token-log review
LICENSE	FREE

Recipe: one delegation, start to finish

1. Read the row: name, client ID, scopes.
2. Token log, 30 days: distinct impersonated users, calls per day, source IPs, scopes actually requested.
3. Token log, activity events, 7 days: API and method names. Reads only, or writes?
4. First-seen probe: sample one-day windows at 180, 90, 60, 30 days back. Present at 180 means older than the log.
5. Admin audit, 180 days: `AUTHORIZE_API_CLIENT_ACCESS` and `REMOVE_API_CLIENT_ACCESS` name the admin who added or changed it, if it was in the window.
6. Match to a product by scope list and method pattern, then confirm with the owner or the vendor's docs.
7. Cloud Console: which project, which organization, who owns it, how many keys, created when.
8. Decide: keep as is, rename, trim scopes, re-key, or remove. Write the decision next to the row.

Gate: every row has a named owner and a one-line purpose; no row has zero events in 180 days; every service account's project is organization-owned; no key is older than the expiry policy; no connector or provisioning job runs as a person or the break-glass.

Gotchas

- **The display name is whatever someone typed.** A project named after a dead product can be running your most important backup. Trust the method names, not the label.
- **Dormant does not mean harmless.** A delegation nobody uses is still a key somewhere nobody is watching. Remove it; re-adding takes a minute.
- **Volume spikes after mass directory changes.** Backup and sync products re-crawl permissions and history when thousands of users change OU or state. Check the product's own log before calling it an incident.
- **A capped query lies about time.** Reports API results are newest-first; 60,000 rows from a 7-day query can all be from this morning. Count per day in separate windows.
- **Read-only scope variants may not be delegated.** A key authorized for the read-write directory scope is refused the read-only scope. Request the scope that is actually listed.
- **The person-shaped integration hides real activity.** A connector making 800 calls a day as a named admin means a real login by that admin is one line in a thousand. Move it off the person before you build alerts.
- **Keys in transcripts.** Any tool that prints a file to a log, a chat, or an AI session has copied the key. Treat a key that has been displayed as burned, and rotate it.

Phase 3b: Student misuse controls

These close the tricks students use to bypass filters, hide activity, cheat, or harass.

Almost all are Chrome user/browser policies applied to the Students OU under **Devices**

> **Chrome** > **Settings** > **Users & browsers**, so they follow the student account on any enrolled device.

Filter and monitoring bypass

☐ Google Lens: all five policies off

SET TO	Google Lens: Disabled across all five Lens policies (see recipe below)
WHY	Lens screenshots a page and searches it, which turns any image, PDF, or blocked page into a search box that filters can't see. The fastest cheating tool on a Chromebook.
WHERE	Users & browsers > search "Lens" (Overlay, region search, camera assisted search, Gallery integration, New Tab button)
LICENSE	

☐ Google Translate

SET TO	Google Translate: block <code>*.translate.goog</code> and <code>translate.googleusercontent.com</code> only; keep <code>translate.google.com</code> and the Chrome translate bar on
WHY	The website-translation proxy runs on <code>translate.goog</code> , not on the app's domain. Blocking the app breaks ELL students and world-language classes for no security gain. The in-page translate bar never proxies; locked mode disables it for quizzes.
WHERE	Users & browsers > Content > URL blocking
LICENSE	

☐ Cached pages, AMP, and web archives

SET TO	Cached pages, AMP, and web archives: block exactly <code>webcache.googleusercontent.com</code> , <code>web.archive.org</code> , <code>*.ampproject.org</code> (students only)
WHY	Same proxy trick. Google's cache is retired, so that entry is near-zero risk, but never widen it: <code>*.googleusercontent.com</code> breaks Docs images, Drive, Sites, and Apps Script. Leave <code>web.archive.org</code> open for staff; teachers use it for research.
WHERE	Users & browsers > Content > URL blocking
LICENSE	

☐ Incognito mode

SET TO	Incognito mode: Disallow incognito mode (already the K-12 default; confirm it); Browser history: Always save ; Clear browser history: Do not allow
WHY	No activity should be invisible to monitoring tools. Chrome won't close Incognito windows already open, so the policy lands on the next restart.
WHERE	Users & browsers > Security > Incognito mode / Browser history / Clear browser history
LICENSE	CEU

☐ Sign-in to secondary accounts

SET TO	Sign-in to secondary accounts: Block users from signing in to or out of secondary Google Accounts
WHY	A personal Google account added in-session bypasses every OU setting. This is the ChromeOS in-session control; the device-level Sign-in restriction covers the login screen.
WHERE	Users & browsers > Sign-in settings > Sign-in to secondary accounts
LICENSE	CEU

☐ Automatic sign-out across devices

SET TO	Automatic sign-out across devices: Automatically sign out user from previous device
WHY	One account on one Chromebook at a time. Google's own description names the school use case: stops shared credentials for collaboration and cheating on graded work.
WHERE	Users & browsers > Sign-in settings > Automatic sign-out across devices
LICENSE	CEU

☐ Developer tools off, chrome:// pages blocked

SET TO	Developer tools: Never allow ; block <code>chrome://flags</code> , <code>chrome://policy</code> , <code>chrome://extensions</code> , <code>chrome://settings/*</code> as needed
WHY	Dev tools and flags are how students disable extensions and rewrite page content.
WHERE	Users & browsers > User experience > Developer tools; URL blocking
LICENSE	CEU

☐ Extensions: allowlist only

SET TO	Extensions: allowlist only; block installs from outside the list. Add the web filter's and classroom-monitoring extension IDs to the allowlist and force-install list first
WHY	VPN and proxy extensions are the #1 filter bypass. Flipping to allowlist-only without the filter's ID removes the filter.
WHERE	Devices > Chrome > Apps & extensions > Users & browsers > Additional settings
LICENSE	CEU

☐ Force SafeSearch; YouTube Restricted Mode via Chrome policy

SET TO	Force SafeSearch; YouTube Restricted Mode via Chrome policy: At least Moderate for all student OUs, Do not enforce for staff
WHY	Browser-level header on every YouTube request, signed in or not; the backstop if the filter extension crashes. Strict hides a lot of legitimate educational video, and layered restrictions (Chrome header + GoGuardian + DNS restrict.youtube.com) resolve to the strictest, so keep Chrome at Moderate and let the web filter carry Strict and any per-class or time-based exceptions. One source of truth per job.
WHERE	Users & browsers > Content > SafeSearch and Restricted Mode
LICENSE	CEU

☐ YouTube account setting

SET TO	YouTube account setting: Strict + approved videos for K-8 (teachers as approvers), Moderate for 9-12, Unrestricted for staff
WHY	Account-level control that follows the student. Approved videos let teachers whitelist specific content. If the Chrome policy is Strict, it overrides approvals, so keep the Chrome policy at Moderate for any OU that relies on approved videos. Test one approved video as a student before rollout.
WHERE	Apps > Additional Google services > YouTube > Content settings / Permissions
LICENSE	FREE

☐ Safe Browsing Protection Level

SET TO	Safe Browsing Protection Level: Standard for students, Enhanced for staff; users can't override warnings; never "user decides" or "never active"
WHY	Standard checks URLs against threat lists with privacy-preserving hashing. Enhanced sends full URLs, page snippets, and downloads to Google tied to the account, which is a student-data-privacy question for minors but a clear win for staff, who are the phishing targets.
WHERE	Users & browsers > Security > Safe Browsing
LICENSE	CEU

❑ Local file blocking

SET TO	Local file blocking: in the web filter (GoGuardian, Securly, etc.), block <code>file:///*/downloads/*.html</code> , <code>*.mhtml</code> , <code>*.mp4</code> , <code>*.mkv</code> , <code>*.mp3</code> and <code>file:///media/removable/*.html</code> , <code>*.mhtml</code> ; in the Chrome URL blocklist , add <code>file:///media/removable/</code> as a plain prefix
WHY	A downloaded games hub or saved page opens from Downloads as a local file where no filter sees a request; downloaded video sidesteps YouTube Restricted Mode. The filter's matcher supports wildcards anywhere in the URL; Chrome's URL blocklist only wildcards the host and prefix-matches the path, so it cannot match by file extension, and the ChromeOS Downloads path contains a per-user hash that can't be prefixed. The removable-media prefix is the one part Chrome policy can hold on its own.
WHERE	Web filter rules; Users & browsers > Content > URL blocking
LICENSE	CEU FILTER

❑ Google Apps Script

SET TO	Google Apps Script: Off for students
WHY	Students deploy Apps Script web apps as game launchers and proxies on <code>script.googleusercontent.com</code> , a Google domain filters trust. Removing the service is more durable than any detector.
WHERE	Apps > Google Workspace > Service status > Apps Script (it became a core service in June 2026 and may not yet appear in the sidebar or under Additional Google services; use Service status or the Admin console search box). If absent, API controls blocking unconfigured apps is a partial stopgap; the anti-evasion extension's Apps Script inspector covers the rest.
LICENSE	FREE

❑ Force-install an anti-evasion extension

SET TO	Force-install an anti-evasion extension (e.g., You Shall Not Pass by TeacherMagic.org, free) alongside the network filter
WHY	Blocks proxy frameworks (Ultraviolet, Scramjet, Rammerhead), Google Sites game hubs, tab spam, and history-flood attacks the network filter can't see. One layer, not a replacement.
WHERE	Devices > Chrome > Apps & extensions > Users & browsers > Add from Chrome Web Store, Force install; https://chromewebstore.google.com/detail/you-shall-not-pass-by-tea/efggnkbeomjjanjmghbadgggegjemogee
LICENSE	CEU

☐ YSNP: Strict Sites and managed config

SET TO	If using YSNP: enable Strict Sites mode and host a managed config JSON before rollout
WHY	Default-deny iframe allowlist on Google Sites defeats obfuscation; the managed config is the kill switch for false positives without waiting on a store release.
WHERE	Extension policy in Apps & extensions; district-hosted JSON
LICENSE	CEU

☐ Task manager

SET TO	Task manager: Block users from ending processes with the Chrome task manager
WHY	Killing the filter extension's process disables it. Users can still open the task manager; End process is dimmed.
WHERE	Users & browsers > Apps and extensions section > Task manager
LICENSE	CEU

Optional: stop students from changing their own passwords

Use these only if the district sets student passwords (for example, synced from the SIS). If students manage their own passwords by policy, skip this block.

☐ Block the password-change pages

SET TO	URL blacklist: myaccount.google.com/signinoptions and myaccount.google.com/smartlink/password (Students OU)
WHY	Blocks the Google Account password-change page, and the passkey pages beneath /signinoptions . Limits: only works in managed Chrome; does not touch the "Forgot password?" flow; does not undo passwords already changed. The /signinoptions prefix match is not documented by Google, so verify with a test student that /signinoptions/password is blocked.
WHERE	Devices > Chrome > Settings > Users & browsers > Content > URL blocking
LICENSE	CEU

☐ Passkey sign-in

SET TO	Passkey sign-in: Off for Students ("Allow users to skip their password and authenticate with a passkey" unchecked). Google default is Off, so confirm it is inherited rather than overriding.
WHY	Otherwise a student can add a passkey and bypass the SIS-set password. Does not apply if students sign in through a third-party IdP. If Staff go passwordless with security keys, turn it on as a Staff OU override, never at root. The Passkeys Restriction card on the same page ("hardware security keys only") is the Staff enforcement for key-only 2SV; enable it only after User reports > Security shows every staff key enrolled.
WHERE	Security > Authentication > Passwordless > Skip passwords card
LICENSE	FREE

☐ Self-service account recovery

SET TO	Self-service account recovery: Off for Students ("Allow users and non-super admins to recover their account" unchecked)
WHY	Closes the reset-by-recovery-phone path. Google notes this setting does not apply when SSO or Password Sync is in use.
WHERE	Security > Authentication > Account recovery
LICENSE	FREE

Recipe: disabling Google Lens (and the settings that go with it)

Lens is not one setting. In the Admin console it is five separate Chrome policies, and a sixth surface (the website) that no policy covers. Search "Lens" in Users & browsers settings with the Students OU selected and set all five; missing one leaves an entry point.

Path: Devices > Chrome > Settings > Users & browsers > select the **Students** OU (and any assessment OU) > search "Lens"

SETTING	VALUE	WHAT IT CLOSES
Google Lens Overlay	Do not allow Google Lens overlay	The address-bar and side-panel Lens that screenshots the current page. This is the main cheating entry point.
Google Lens region search	Disable Google Lens region search	Right-click > "Search with Google Lens" on any image or selected region.
Google Lens camera assisted search	Do not allow enterprise user to use Google Lens camera assisted search	Pointing the Chromebook camera at a worksheet from the Lens shortcut.
Lens Gallery App integration	Disable Lens integration (user override not allowed)	The Lens button inside the ChromeOS Gallery app, which handles downloaded images and PDFs.
New Tab page Google Lens button	Do not show the Google Lens button in the search box on the New Tab page	The camera icon in the new-tab search box.
URL blocklist: lens.google.com , images.google.com/searchbyimage	Add	Lens is also a website. The browser policy doesn't block the site.
Camera app on ChromeOS	Block during assessments via a kiosk or locked-mode OU; otherwise leave on	The ChromeOS Camera app can scan text and QR codes. Only worth blocking in an assessment OU, since teachers use it for projects.
Quick Answers	Disabled	Highlighting a word on ChromeOS pops up definitions, translations, and unit conversions without opening a tab. Same cheating surface as Lens, smaller. Users & browsers > Content > Quick Answers.
Side search / Google side panel	Disabled	Lets a student search without leaving the assessment tab. Users & browsers > User experience > Side search.
Default search context menu ("Search Google for ...")	Disabled	Highlight a question, right-click, get the answer. Users & browsers > Content > Default search provider context menu.
Screenshots	Disabled for assessment OUs	Students screenshot a test to share, or to feed to an AI on a phone. Users & browsers > Content > Screenshot.
Google Forms locked mode	On for quizzes on managed Chromebooks	Locks the quiz to one tab, blocks extensions, and Google turns off Lens, Translate, and side panel automatically for that session. Teacher-side setting in Forms; requires enrolled Chromebooks.

Notes:

- **Web filter interplay.** None of the Chrome policies in this phase conflict with GoGuardian, Securly, Lightspeed, or iBoss; most of them protect the filter extension. Two exceptions: the Screenshots policy breaks classroom screen monitoring, and the extension allowlist must include the filter before enforcement. For YouTube, three layers can stack (Chrome header, filter policy, DNS restrict.youtube.com); the strictest wins and teacher-approved videos fail silently, so pick one layer to carry Strict.
- Apply Lens Disabled to the whole Students OU, not just an assessment OU. Students use it to solve homework at home just as easily.
- Third-party AI and homework-answer sites (photo-solver apps, answer aggregators) are the same threat outside Google; block the "Generative AI" and "Academic dishonesty" categories in the web filter.
- Staff keep Lens. It's a legitimate accessibility and research tool.

Phase 3c: Turning off AI for student OUs

Google's 18+ restriction on Gemini in Workspace apps does most of this automatically once the under-18 age label is set, but several AI surfaces are controlled separately and default to on. Set every one of these explicitly at the Students OU; do not rely on inheritance. All Gemini controls live under the top-level **Generative AI** menu in the Admin console (Gemini app, Gemini Enterprise, Gemini in Workspace, Gemini Notebook, Gemini reports), not under Additional Google services.

Workspace AI (Admin console)

☐ Gemini app

SET TO	Off
WHERE	Generative AI > Gemini app (Students OU)
LICENSE	FREE

☐ Gemini conversation sharing and Gem sharing

SET TO	Off: no conversation sharing by public link or Drive; "Allow people to share Gems from the Gemini app" off. Set it even with the Gemini app off, so it is already closed if Gemini is turned on for a grade
WHERE	Generative AI > Gemini app > Sharing (Students OU)
LICENSE	FREE

☐ Gemini temporary chats and conversation deletion

SET TO	Off: "Allow temporary chats" and "Allow users to delete conversations" both unchecked. Temporary chats skip Gemini Apps Activity, and deletion erases evidence after a cheating or safety incident. For records you can produce, add a Vault retention rule for Gemini; Vault keeps data regardless of user deletions
WHERE	Generative AI > Gemini app > Gemini conversation management (Students OU)
LICENSE	FREE

☐ Gemini in Workspace

SET TO	Off per app
WHERE	Generative AI > Gemini in Workspace (Students OU)
LICENSE	FREE (Plus controls each app separately)

☐ Gemini Notebook / NotebookLM

SET TO	Off
WHERE	Generative AI > Gemini Notebook (Students OU)
LICENSE	FREE

☐ Gemini Notebook sharing outside of Students

SET TO	OFF ; Public Sharing unchecked. Never ON: Google notes that when notebooks are shared with consumer users, their feedback (sources, queries, responses, artifacts) can be used for human review and model training. Use ALLOWLISTED DOMAINS only for a documented partner-school need. Set it even while NotebookLM is off, so it is locked when 9-12 gets access
WHERE	Generative AI > Gemini Notebook > Sharing > Sharing outside of Students (Students OU)
LICENSE	FREE

☐ Gemini Enterprise

SET TO	Off
WHERE	Generative AI > Gemini Enterprise (Students OU)
LICENSE	ADD-ON

☐ Gemini reports

SET TO	Verify zero student usage after the above
WHERE	Generative AI > Gemini reports, filtered to Students OU
LICENSE	FREE

☐ Workspace Studio

SET TO	Off
WHERE	Agents menu, or Apps > Google Workspace > Workspace Studio (Students OU)
LICENSE	FREE

☐ Google Vids

SET TO	Off unless a teacher requests it for a specific OU
WHERE	Apps > Google Workspace > Vids > Students OU
LICENSE	FREE

☐ Meet "Take notes for me" and AI summaries

SET TO	Off
WHERE	Apps > Google Workspace > Google Meet > Gemini features > Students OU
LICENSE	FREE

☐ Gemini in Classroom

SET TO	Keep On for staff , verify Off for students
WHERE	Apps > Google Workspace > Classroom > Gemini
LICENSE	FREE

☐ Third-party AI apps

SET TO	Blocked via API controls; do not allowlist for students
WHERE	Security > Access and data control > API controls
LICENSE	FREE

Chrome AI (Chrome policy, Students OU)

☐ Generative AI section

SET TO	Disabled / Do not allow, each setting
WHERE	Users & browsers > Generative AI (its own section; search "Generative AI")
LICENSE	CEU

☐ Gemini in Chrome

SET TO	Disabled
WHERE	Users & browsers > Generative AI > Gemini integrations
LICENSE	CEU

☐ Google Lens (five policies)

SET TO	Disabled
WHERE	See recipe above
LICENSE	CEU

☐ Google Search AI Mode

SET TO	Block google.com/aimode in URL blocklist; the age label also restricts AI Mode for under-18 accounts, and the web filter should block the query-param variant
WHERE	Users & browsers > Content > URL blocking
LICENSE	CEU FILTER

☐ Third-party AI sites

SET TO	Block "Generative AI" category
WHERE	Web filter console
LICENSE	FILTER VENDOR

Verify

Sign in as a test student on an enrolled Chromebook and confirm: no Gemini star in Docs or Gmail, no Lens on right-click, no AI Mode tab in Google Search, gemini.google.com and notebooklm.google.com blocked, Help me write absent in Chrome text fields. Repeat after each Chrome and Workspace release; AI entry points are added monthly.

Gate: test student passes the verification above; staff Gemini confirmed still working.

Device-side hardening (Chromebooks)

☐ Android apps (Play Store)

SET TO	Android apps (Play Store): Off for students
WHY	Sideloaded and Play-store VPNs, browsers, and games.
WHERE	Devices > Chrome > Apps & extensions > Users & browsers > Play Store
LICENSE	CEU

❑ Linux virtual machines for users

SET TO	Linux virtual machines for users: Block usage of Virtual Machines needed to support Linux apps (Students OU); also block "Linux virtual machines for unaffiliated users" on the Device settings tab
WHY	A Linux container is a full shell with network access outside every browser policy and the filter extension; a student can run a local proxy and point Chrome at localhost. When blocked, the "Linux development environment" toggle disappears from the Chromebook's Settings > Advanced > Developers. Allow only for a CS OU that teaches with it.
WHERE	Users & browsers > Virtual machines > Linux virtual machines for users; Device settings > Virtual machines
LICENSE	CEU

❑ External storage

SET TO	External storage: Read-only or disabled
WHY	Blocks booting alternate OS images and offline file transfer.
WHERE	Devices > Chrome > Settings > Device > External storage
LICENSE	CEU

❑ Video input (camera)

SET TO	Video input (camera): Do not allow sites to access the camera for grade bands where proxied video chat is a problem (one district did this for middle school after students reached Omegle-style sites through proxies); leave Audio input (microphone) alone unless the same problem applies
WHY	Camera and microphone are two separate Chrome user policies, set per OU; the device inherits from its parent, so select the exact OU before changing it. Blocks all video input through Chrome and web apps, external webcams included. Impact: Google Meet video and Clever Badge (QR card) logins stop working for that OU; use the companion "Video input allowed URLs" list to re-allow meet.google.com and clever.com if those are needed. The ChromeOS Camera app is separate; block it in Apps & extensions if you want that gone too. Allow up to 24 hours to propagate.
WHERE	Users & browsers > Hardware > Video input; Video input allowed URLs; Audio input
LICENSE	CEU

☐ Screen video capture

SET TO Screen video capture: **Do not allow sites to prompt the user to share a video stream of their screen** (Students OU)

WHY A shared screen streams a test, or a whole class period, to someone outside the room, and covers the screen-share half of random video chat the camera setting leaves open. Calls to screen-share APIs fail, including screen-recorder extensions. **Impact:** students can't present in Google Meet or record screencasts (Screencastify, Loom, WeVideo); add meet.google.com and the approved recorder to the "capture allowed by sites" lists on the same page.

WHERE Users & browsers > search "Screen video capture"

LICENSE **CEU**

☐ Screenshots

SET TO Screenshots: **Disabled** only for assessment OUs that don't use classroom monitoring

WHY Blocks capture through extension APIs, which is how GoGuardian Teacher, Securly Classroom, and Lightspeed Classroom show live student screens. Enabling it OU-wide breaks monitoring.

WHERE Users & browsers > Content > Screenshot

LICENSE **CEU**

☐ Powerwash

SET TO Powerwash: **Do not allow powerwash to be triggered**

WHY Powerwash then dev-mode is the classic unenroll attempt (forced re-enrollment catches it, but blocking is cleaner).

WHERE Devices > Chrome > Settings > Device settings > Enrollment and access > Powerwash

LICENSE **CEU**

☐ Chrome Remote Desktop host

SET TO Chrome Remote Desktop host: **Blocked**

WHY Covered in Phase 3; repeated here because it's a student bypass too.

WHERE Users & browsers > Remote access

LICENSE **CEU**

Workspace-side misuse controls

☐ Google Chat: off K-5, internal-only 6-12

SET TO	Google Chat: off for K-5; internal-only, no external spaces for 6-12
WHY	Harassment and off-task chatting. Docs comments and Meet chat are the fallback vectors; monitor them.
WHERE	Apps > Google Workspace > Google Chat
LICENSE	FREE

☐ Offline access off for shared carts

SET TO	Docs/Drive: disable "Offline access" for shared carts
WHY	Prevents cached student data on the next user's session.
WHERE	Apps > Google Workspace > Drive and Docs > Features and Applications
LICENSE	FREE

☐ All AI surfaces

SET TO	All AI surfaces: see Phase 3c
WHY	Gemini, NotebookLM, Chrome AI, Search AI Mode, and third-party AI each have their own switch.
WHERE	Phase 3c
LICENSE	FREE CEU

☐ Google Meet: no student-created or external meetings

SET TO	Google Meet: students can't create meetings, can't join external, "Host management" on by default
WHY	Prevents unsupervised video calls.
WHERE	Apps > Google Workspace > Google Meet > Meet safety settings
LICENSE	FREE

☐ Groups, Sites, Blogger, and Photos off

SET TO	Google Groups: Off ; Sites: Off (creation); Blogger: Off ; Google Photos: Off
WHY	Each is a publishing or messaging surface with weak monitoring. Turning Sites off stops students creating hubs; viewing sites.google.com still works, which is why Strict Sites mode above exists.
WHERE	Apps > Additional Google services
LICENSE	FREE

☐ Contacts: no external directory sharing

SET TO	Contacts: block external directory sharing
WHY	Stops harvesting staff and student emails.
WHERE	Apps > Google Workspace > Directory > Sharing settings
LICENSE	FREE

☐ Investigation tool alerts on mass sharing, mass deletion, and suspicious Drive activity

WHY	Surfaces harassment documents and cheating rings early.
WHERE	Security > Security center > Investigation tool; Rules
LICENSE	PAID

Gate: pilot classroom runs one full week with the filter vendor confirming no bypass; teachers report no lost instructional tools.

Appendix: Additional Google services checklist for the Students OU

Path: Apps > Additional Google services, with the Students OU selected. Every service showing "Inherited" is taking the root setting; set explicit overrides here so staff are unaffected. Anything left On for students requires annual parental-consent reconfirmation in this same list (Google turns it off for under-18 users if you don't), so a short On list is also less yearly work. Google Apps Script is not in this list; it became a core service in June 2026 and is managed from Apps > Google Workspace > Service status (it may not yet show in the sidebar on every tenant). Set it Off for students.

SERVICE	STUDENTS	WHY
Google Cloud Platform	Off	Free-tier VMs and Cloud Run are where students host proxies. The single most important one in this list.
Colab	Off (allow a CS OU if needed)	Arbitrary code with outbound network; tunnels and proxies run fine from a notebook.
AI Studio	Off	Gemini API playground. Belongs with the Phase 3c AI shutoff.
Chrome Web Store	Off	Students are on an extension allowlist anyway; this removes the browse-and-request surface. Force-installed extensions still update via policy.
Google Play, Managed Google Play	Off	Matches the Play Store Off Chrome policy.
Messages by Google	Off	Texting from a Chromebook via messages.google.com.
Google Photos, Blogger, Google Groups	Off	Publishing and messaging surfaces with weak monitoring.
Early Access Apps	Off	New Google products appear for students before review.
Google Pay, Google Fi, Brand Accounts, Google Domains, Business Profile Manager	Off	No student use case.
Google Ads, Ad Manager, Campaign Manager, Merchant Center, Search Console, Programmable Search Engine, Play Console, Play Books Partner Center, Partner Dash, FeedBurner, Google Analytics, Tag Manager, Search Ads 360	Off	Advertiser and publisher tools; no K-12 student use.
Google Developers, Material Gallery, Pinpoint, Google Alerts, Google Bookmarks, Question Hub, Studio, Tables	Off	Low risk, no use. Shrinks the surface.
Scholar Profiles	Off	Creates a public academic profile page under the student's name. Privacy exposure, no K-12 use. Google Scholar search itself stays on.
Search and Assistant	Off	Signs students out of Search personalization, disables Google Assistant on Chromebooks, and removes account-tied AI Mode and search history. Search still works as a signed-out service.
Socratic	Off	Photo-a-homework-question solver.
Timeline	Off	Maps location history. Data collection, not a feature.
Data Studio (Looker Studio)	Off unless a data or business class uses it	Judgment call.
Chrome Remote Desktop	Off	Covered in Phase 3.
Web & App Activity, Location History	Off	Data-collection settings, not features.
Third-party app backups	Off	Lets non-Google apps (WhatsApp, some Android apps) store hidden backups in the account's storage. Not an attack surface; it's invisible storage use and personal app data in a district account that no admin tool can retrieve. Low priority.

SERVICE	STUDENTS	WHY
YouTube	Configure per the Restricted Mode rows in Phase 3b	Do not leave inherited.
Google Maps, My Maps, Google Earth, Arts and Culture, Google Books, Google News, Public Data, Google Scholar	On	Instructional.
Google Translate	On	ELL and world-language classes; the proxy is blocked separately by hostname.
Chrome Canvas, Chrome Cursive, Applied Digital Skills, CS First	On	Harmless or Google's own curriculum.

Phase 3d: Seams the review surfaced

These close the gaps between the two directories, between "detect" and "respond", and inside the threat model itself: delegated roles that are super admin in everything but name, sessions that outlive the factor that opened them, three external surfaces DLP never sees, and Gemini as a first-party agent sitting inside the tenant with Drive and Gmail reach. Everything here is per OU, and nearly all of it is free.

Admin roles, sessions and the help desk

☐ Audit delegated admin roles by what they can do, not by the super-admin label

SET TO	Export every admin role assignment (pre-built and custom) with the OUs it covers. Flag any role holding User Management privileges — password reset, 2-Step Verification reset, security-key management — over staff or admin OUs.
WHY	A helpdesk role that can reset a super admin's daily-driver password is effectively super admin. Counting super admins while ignoring these is an incomplete audit.
WHERE	Account > Admin roles > each role > Admins and Privileges; export with GAM print admins
LICENSE	FREE

☐ Scope password and 2SV resets to student OUs for helpdesk roles

SET TO	Helpdesk custom role: User Management privileges limited to the Students OU tree. Staff and admin resets require a separate, security-key-protected admin account held by two named people.
WHY	A phone call to the helpdesk should never be able to take over a staff or central-office account. This is the technical half of the verification procedure below.
WHERE	Account > Admin roles > Create new role > Privileges > assign to the Students OU only
LICENSE	FREE

☐ Written help-desk verification procedure, rehearsed

SET TO	No password reset, 2SV reset or security-key enrollment for admin, finance, HR or central-office accounts by phone, ever; callback to the number on file or a shared verification word for everyone else; every reset logged with the method used.
WHY	Scattered Spider's path was a help-desk call. Voice cloning needs three seconds of audio, and the caller can now be an agent. The vishing simulation grades this procedure, not the person.
WHERE	Written procedure; reviewed weekly against the admin audit log (USER_PASSWORD_CHANGED, 2SV events)
LICENSE	FREE

☐ Re-authentication for sensitive admin actions

SET TO	Admin console reauthentication policy on, with the security key as the method; Google Cloud session control for admins at 1 to 4 hours.
WHY	Session cookies get stolen after MFA (infostealers), not instead of it. Re-auth on admin actions means a replayed cookie still cannot change the tenant.
WHERE	Security > Authentication > Google session control; Security > Authentication > Reauthentication policy
LICENSE	FREE

☐ Alert on role changes and on resets of staff or admin accounts

SET TO	Activity rule or saved alert on ASSIGN_ROLE / UNASSIGN_ROLE, and on password or 2SV changes for accounts in staff and admin OUs.
WHY	Role assignment is the quiet way to keep access after a password reset. Resets of admin accounts outside business hours are an incident until proven otherwise.
WHERE	Security > Alert center > rules; Reporting > Audit and investigation > Admin log events
LICENSE	FREE (system alerts); PAID (custom activity rules)

External surfaces DLP on Drive never sees

☐ Groups for Business — no public groups, external members off

SET TO	Sharing options: group visibility inside the domain only; creating public groups not allowed; external members not allowed by default, owners cannot override for student OUs; posting from outside not allowed.
WHY	A group that accepts outside posts or members is an inbox nobody owns and an exfil list nobody audits.
WHERE	Apps > Google Workspace > Groups for Business > Sharing settings
LICENSE	FREE

☐ Calendar free/busy only outside the domain

SET TO	External sharing options: Only free/busy information (hide event details); internal sharing per OU; secondary calendars inherit.
WHY	Event titles and descriptions carry names, locations and sometimes credentials; free/busy carries none of them.
WHERE	Apps > Google Workspace > Calendar > Sharing settings > External sharing options
LICENSE	FREE

☐ Chat external off for students, allowlisted for staff

SET TO	Students: external chat off. Staff: external chat allowed only with allowlisted domains; file sharing in external spaces off; Chat apps restricted to allowlisted apps.
WHY	Chat is a file-transfer and link-delivery path that DLP on Drive never sees, and an external space is an injection channel into any staff member's Gemini.
WHERE	Apps > Google Workspace > Google Chat > External chat settings; Chat apps
LICENSE	FREE

☐ Chrome extension allowlist for staff, not only students

SET TO	Apps & extensions for the staff OU: block all, allowlist by extension ID; review host permissions on every allowlisted extension; block AI browser-agent extensions explicitly (Claude in Chrome, Comet, Atlas and similar); extension install reporting on.
WHY	An extension rides the already-authenticated session, past security keys and Context-Aware Access. It inherits everything the user can reach, and a prompt-injected browser agent is an insider with a mouse.
WHERE	Devices > Chrome > Apps & extensions > Users & browsers > Staff OU; Allow/block mode = Block all; Reporting > Chrome extension list
LICENSE	FREE (managed Chrome browser or ChromeOS); CEU on Chromebooks

Gemini and NotebookLM as first-party agents

☐ Gemini for Workspace decided per OU, staff included

SET TO	Gemini (the app) and Gemini in Gmail, Drive, Docs, Sheets, Slides and Meet: on only for OUs that use it; off for central-office and finance/HR OUs that hold high-value data; never inherited On by default.
WHY	Gemini is a first-party agent with the user's Drive and Gmail reach. A shared document with injected instructions, opened by a staff member whose Gemini is on, is the lethal trifecta — private data, untrusted content, a way out — pre-assembled inside the tenant.
WHERE	Apps > Google Workspace > Gemini app; Apps > Google Workspace > each app > Gemini features; per OU
LICENSE	FREE to turn off; feature availability by edition

☐ NotebookLM sharing inside the district only, off where unused

SET TO	NotebookLM service on only for OUs that use it; sharing of notebooks restricted to the domain; students per Phase 3c.
WHY	A notebook aggregates sources into one exportable surface; external sharing of it is bulk export with a friendly name.
WHERE	Apps > Additional Google services > NotebookLM; Sharing settings
LICENSE	FREE

☐ Reduce how often an injected document reaches a staff Gemini

SET TO	External sharing into staff Drives limited (Phase 3 sharing settings); Gmail external-sender banners on; Drive 'Warn when sharing outside' on; shared-drive creation restricted.
WHY	You cannot patch prompt injection; you can reduce the untrusted-content leg. Google publishes layered mitigations for indirect injection against Gemini; the admin's part is limiting which OUs give the agent all three legs at once.
WHERE	Apps > Google Workspace > Drive and Docs > Sharing settings; Gmail > Safety
LICENSE	FREE

Data, logs, response and restore

☐ Custom DLP detectors and Drive labels for district data

SET TO	Drive labels (Student Records, Special Education, Health, Discipline) applied by owner or by DLP; custom detectors (regex / word lists) for IEP, 504, discipline and grade-export shapes; rules target the label, not all of Drive.
WHY	Predefined detectors are SSN- and card-shaped. The data that matters in a district — IEPs, discipline, grades, health — mostly is not. Labels let the rule find it.
WHERE	Security > Access and data control > Data protection > Manage detectors; Apps > Drive and Docs > Labels
LICENSE	PAID

☐ Vault export privileges on dedicated roles, alert on every export

SET TO	Vault privileges (Manage Matters, Manage Exports, Manage Searches) held only by a dedicated records/legal admin role, never bundled onto a daily account; saved alert on every Vault export event.
WHY	Vault is built to search every mailbox and Drive and export the result. In the wrong hands it does not leak data; it exports the district. A legitimate export is rare and planned; a surprise one is an incident.
WHERE	Account > Admin roles > Vault privileges; Reporting > Audit and investigation > Vault log events > create alert
LICENSE	FREE (included in Education Fundamentals)

☐ Export audit logs beyond Google's retention

SET TO	BigQuery export of Workspace logs (Education Standard/Plus) or a scheduled GAM/Reports API pull into Wazuh; keep at least 18 months.
WHY	Most Workspace audit logs are retained about six months. Agent-assisted intrusions compress the attack but can still be discovered late; you need the log to still exist.
WHERE	Reporting > Data export (BigQuery); Reports API activities.list via GAM
LICENSE	PAID (BigQuery export); FREE (GAM pull)

❑ Automated response on the never-legitimate rules

SET TO	Activity rules with the Suspend user action on: external-forwarding rule created, mass download, new domain-wide delegation, Vault export outside the records role. Tabletop the false-positive path once.
WHY	At 2 AM on a holiday an alert with no action is an audit log. Machine-speed attacks get machine-speed response on the handful of rules that are never legitimate.
WHERE	Security > Alert center > Activity rules > Actions
LICENSE	PAID (custom activity rules)

❑ Tested restore of Gmail and Drive, with a measured RTO

SET TO	Twice a year: restore one user's Drive and mailbox from Vault (25-day window) and from the third-party backup; restore a shared drive; time it and write the RTO down.
WHY	A restore you have never run is a hope. Google's own recovery window is short; your backup product's restore has probably never been tried under pressure.
WHERE	vault.google.com ; backup console; runbook
LICENSE	FREE (Vault); PAID (third-party backup)

Gate: every admin role exported with its OU scope and reviewed; no role outside the two named admin accounts can reset a staff or admin password; Gemini decided per OU in writing; one Vault export alert and one activity rule with an action tested; one restore timed.

Gotchas

- **Session length and Mac logins.** Shorter sessions re-prompt Mosyle Auth / Jamf Connect users; keep staff at 12 to 24 hours and apply the short session to admin accounts only.
- **Blocking all extensions breaks the filter.** Allowlist your content filter, screen-management and accessibility extensions before switching the staff OU to Block all; test on one building.
- **Gemini off is per app, not one switch.** The Gemini app and Gemini features inside Gmail, Drive, Docs and Meet are separate settings and inherit separately; verify each one on a test account in the OU.
- **Suspend-user actions need a human path.** A rule that suspends the superintendent at 7 AM on a false positive needs a documented un-suspend procedure and a second admin who can run it.
- **Vault export alerts fire on legal's work too.** Name the records role in the rule's exclusion, or accept that every legitimate export is a two-minute acknowledgment.

Phase 4: Keep it that way

☐ Alert rules for sharing, CAA, logins, OAuth

SET TO	Alert rules: external sharing spike, CAA denials, suspicious logins, new OAuth grants
WHY	You find out the day it happens, not at audit time. Every edition can read the raw logs at Reporting > Audit and investigation; Education Plus adds the Security center, the investigation tool, and the ability to turn a saved search into an alert rule.
WHERE	Rules (top-level menu) or Security > Alert center; Reporting > Audit and investigation > [source] log events
LICENSE	FREE (built-in system alerts); PAID (custom activity rules built from the investigation tool)

☐ Monthly Security Health review

WHY	Google flags drift for you.
WHERE	Security > Security center > Security health
LICENSE	PAID

☐ Quarterly Security advisor review

SET TO	Quarterly Security advisor review (recommended settings, app access protection, data protection)
WHY	Google's own checklist of settings it thinks you should turn on; cheap way to catch anything this guide misses.
WHERE	Security > Security advisor
LICENSE	FREE

☐ Quarterly prune of approved devices and enrolled Chromebooks

WHY	Old devices are unmonitored back doors.
WHERE	Devices > Mobile & endpoints > Devices / Devices > Chrome > Devices
LICENSE	FREE

☐ Quarterly shared-drive and public-file audit

SET TO	Quarterly shared-drive and public-file audit (see recipe in Phase 3)
WHY	Old shared drives keep the sharing settings they were created with; public links accumulate.
WHERE	Apps > Drive and Docs > Manage shared drives; GAM
LICENSE	FREE

☐ Annual under-18 consent reconfirmation

SET TO	Annual under-18 consent reconfirmation for every Additional Google service left On for students
WHY	Google requires Education admins to re-confirm parental consent for under-18 access yearly; services not reconfirmed are turned off for students automatically, usually mid-year, and teachers notice first.
WHERE	Apps > Additional Google services; check the box next to each app or use the three-dot menu to reconfirm
LICENSE	FREE

☐ Monthly check that the travel-exception group is empty

WHY	Exceptions should expire.
WHERE	Directory > Groups
LICENSE	FREE

☐ Quarterly review of Chrome policy for new bypass vectors

SET TO	Quarterly review of Chrome policy for new bypass vectors (new Chrome features ship monthly)
WHY	Lens, AI features, and Translate all shipped as bypasses after the fact.
WHERE	Devices > Chrome > Settings
LICENSE	CEU

☐ Stage new blocking extensions 5% > 25% > 100%

SET TO	Stage any new blocking extension 5% > 25% > 100% with managed-config kill switches ready
WHY	False positives on state testing or assistive tech are the fastest way to lose teacher trust.
WHERE	Devices > Chrome > Apps & extensions
LICENSE	CEU

☐ Start and end of year: devices and accounts

SET TO	Start/end-of-year: enrollment device assignment, withdrawal suspension, graduate deprovisioning
WHY	Accounts and devices follow students, not the other way around.
WHERE	Directory › Users / SIS sync
LICENSE	FREE

What you can do today, before any upgrade

All FREE and CEU items from Phases 0, 1, 3, 3b, 3c, and 4. In rough priority order:

1. OU restructure, break-glass admin, staff 2SV with keys
2. Age-based access, Chrome Remote Desktop off, Takeout off
3. Student Chrome policies (Lens, Translate, Incognito, multiple sign-in, dev tools, extensions allowlist) and the Phase 3c AI shutoff
4. API controls (trust MDM first), Marketplace restriction
5. Gmail forwarding/POP/IMAP off, safety settings, attachment compliance, student restrict-delivery
6. Drive sharing settings for both lanes
7. Basic mobile management + Device approvals
8. Endpoint Verification pushed to laptops (ready for CAA on day one)
9. Vault retention rules

When the upgrade lands, Phase 2 and the DLP rows are the only new work.

Rollout order

Pilot (IT + one grade band or building) > 6-8 > 3-5 > K-2
> Staff > 9-12

Each step waits for the previous step's gate. If Chromebook device OUs are already per building or cart, staging by building is an equally good alternative to grade band.

Staff vs. Students at a glance

	STAFF	STUDENTS
2SV	Required, keys/passkeys only	Not enforced
Device definition	EV + admin-approved (laptops); Basic management (phones)	Enrolled ChromeOS only
External Drive sharing	Trusted domains	Off
Gmail scope	Open, forwarding blocked	Internal + allowlist
Chat / Meet	Open	Internal only (off for K-5)
DLP action	Warn, then block	Block
Gemini / AI features	Allowlisted	Off
Google Lens / Translate / Incognito	Allowed	Blocked
Third-party apps / extensions	Allowlisted	Allowlisted, stricter
Chrome Remote Desktop	Off (IT OU excepted)	Off
Travel	Group exception	Blocked abroad
Retention	District policy	Student-specific, deprovision on exit

Mac login tools (Mosyle Auth, Jamf Connect, similar)

If Macs sign in through a Google-backed login tool, check these before enforcing anything above:

- ☐ The tool's OAuth clients (login + directory sync) marked **Trusted** in API controls
- ☐ MDM deploys Chrome, EV extension, and EV native helper to every Mac
- ☐ Only **US-Only** assigned to the tool's OAuth app in CAA (no device level)
- ☐ 2SV with security keys tested at the Mac login window; TOTP/Google prompt fallback allowed if keys fail there
- ☐ Session length at least 12h to avoid unlock re-prompts

Admin console paths move between redesigns. If one is wrong, open an issue or PR.