

Chromebook Return & Recovery Audit Checklist

Before devices go out

- ☐ Every device is in the inventory with serial, asset tag, assigned student, and OU
- ☐ Device-to-student assignment is recorded somewhere other than a spreadsheet one person owns
- ☐ Forced re-enrollment is on, so a wiped device returns to your domain
- ☐ Students and families know the report-it-lost process and who to call

First 24 hours after a lost or stolen report

- ☐ Record the report: who, which device, when last seen, police report number if filed
- ☐ Disable the device in Google Admin and confirm the status actually changed
- ☐ Set a disabled-device message with a return contact, so a finder can reach you
- ☐ Sign the student's active sessions out and reset the account password if the device was unlocked
- ☐ Watch for the device checking in again, and decide in advance who acts when it does

End-of-year collection

- ☐ Reconcile devices returned against devices assigned; list every gap by student
- ☐ Deprovision or re-OU returned devices so they stop receiving student policy
- ☐ Chase unreturned devices on a dated schedule, not an open-ended 'we'll follow up'
- ☐ Flag graduating and withdrawn students' devices separately from summer holds

Every month

- ☐ Spot-check a sample of 'returned' devices to confirm they are really in the building
- ☐ Review devices that have not checked in for 30+ days
- ☐ Confirm departed students' accounts are suspended or archived

Want these checks run for you automatically? Visit userauthguard.com.