RESEARCH WHITEPAPER

Student Accountability in 1:1 Programs

What district audits found when nobody owned the device, and how Google Workspace can enforce ownership at the sign-in screen

UserAuthGuard Research · Updated November 2026 · Asan Digital LLC

1. Executive Summary

As 1:1 device programs become standard in K–12 education, schools have to balance the opportunity with sustainable management. This whitepaper sets out what district audits actually found when no one owned the device, and what it takes to make ownership real: not a record of an assignment, but a Chromebook that only its assigned student can sign in to.

> Clear device ownership removes the category of “unexplained” loss: every device has a named holder and a dated history of who held it before.

2. Introduction

By EdWeek Research Center survey figures from 2021, as relayed by device-cart vendor PowerGistics, over 90% of U.S. middle and high schools and 84% of elementary schools run 1:1 device programs **[1]**. These programs expand access, and they create a logistical problem that buying the devices does not solve. “It’s easy to assign a device to a staff member or a student, but it’s trickier to know whether they always have that device,” Louis McDonald, director of technology for Fauquier County Public Schools in Virginia, told Education Week **[2]**.

3. Why Accountability Matters

A record of an assignment is not an assignment. An inventory records what you believed at the moment you wrote it down; it does not stop the device being used by somebody else the next morning. One-to-one assignment that the device itself enforces keeps every Chromebook accounted for continuously, with a dated history of who held it before.

The School District of Altoona in Wisconsin gives students the same device every year. Its director of future-ready learning told Education Week that the practice helps “prolong the life of the device” and helps students know “this is mine to take care of” **[2]**.

4. Fewer Repairs and Accidents

Device-cart vendor PowerGistics says up to 15% of devices can break in a school year, citing sponsored trade-press content rather than a primary survey **[1]**. Treat it as a vendor estimate, not a

benchmark. What is not in dispute is the mechanism: a device with a named holder has someone with a reason to look after it, and a device without one does not. What assigned, enforced ownership changes is the incentive:

- Someone has a reason to avoid the drop, the spill and the backpack with no sleeve
- Minor damage has a person to report it while it is still minor
- A repair bill has a name attached to it

5. Minimizing Lost and Unreturned Devices

These are published findings from district and state audits. They are not our numbers, and none of these districts were UserAuthGuard customers at the time of the audit.

77,505

Chicago Public Schools, 2021–22

Laptops and other tech devices reported lost or stolen in the 2021–22 school year, original purchase price over $23 million, per the district's Inspector General. In the schools that completed a 2022–23 inventory, 11% of tech devices were marked lost or stolen. A later recovery drive found more than 12,000 devices, almost all inside schools, missed in the previous inventory. At three dozen schools, every device assigned to students had been marked lost or stolen. Not all were Chromebooks. **[5]**

22%

20 New York districts, audited 2023

Of 1,155 sampled IT assets, 22% were not properly accounted for, and 11% of them, including 81 Chromebooks, could not be located. None of the 20 districts had policies or procedures specific to IT equipment inventory. **[3]**

11%

Atlanta Public Schools, 2021–22

About 11% of more than 40,000 devices were not returned at the end of the school year. The district expected to spend $3.5 million replacing lost and damaged devices. **[4]**

The common thread across all three is not a missing tracking tool. Chicago, New York and Atlanta all had asset records. What they lacked was a device that knew who it belonged to, and a return anyone was accountable for.

What we do not claim. We do not publish a loss rate, a percentage reduction or a dollar saving for districts using UserAuthGuard. Our customers have not given us before-and-after loss figures, and we will not estimate them on their behalf.

6. How the Assignment Gets Enforced

Google Admin already has the control: **Devices › Chrome › Settings › Device settings › Sign-in restriction**, set to “Restrict sign-in to a list of users”. In Google’s words, “only users that you designate can sign in to devices. Other users get an error message.” **[6]**

The catch is that device settings apply to an organizational unit. Giving one Chromebook to one student means that Chromebook needs its own OU with that student listed: thousands of OUs, edited by hand, redone at every swap. That is why almost no district does it.

UserAuthGuard does that bookkeeping. For each assigned device it creates an OU named by the device’s serial inside a parent “Assigned” OU, sets the allowed user to the assigned student, and moves the device in. Filtering, apps and network settings are inherited from the parent, so policy is still managed in one place; only the allowed user is set per device. Reassign, swap or return the device and the allowed user updates, with a dated history.

Two operational notes: keep guest browsing and managed guest sessions off, because Google notes that with either enabled “users can use devices no matter which setting you choose”, and expect changes to apply within minutes but allow up to 24 hours **[6]**.

7. References

1. PowerGistics, Device Loss and Damage in K–12 (vendor blog; the 1:1 prevalence figures it relays are from EdWeek Research Center, 2021). powergistics.com/blog/device-loss-and-damage/
2. Education Week, Why Schools Struggle to Keep Track of Students’ Laptops, April 2023. edweek.org
3. Office of the New York State Comptroller, Information Technology Asset Management, audit 2022-MS-2, March 2023. osc.ny.gov
4. Atlanta Journal-Constitution, APS to spend $3.5 million replacing devices students lost or damaged. ajc.com
5. Chicago Public Schools Office of Inspector General, FY2023 annual report (January 9, 2024), as reported by WBEZ and Chalkbeat Chicago. wbez.org · chalkbeat.org
6. Google Workspace Admin Help, Set ChromeOS device policies, “Sign-in restriction” (answer 1375678). support.google.com/chrome/a/answer/1375678