USERAUTHGUARD

BLOG CASE STUDIES

How Southeast Delco Manages 9,000 Chromebooks Across 7 Schools

Stef Verleysen | March 14, 2026

> See how Southeast Delco School District transformed its Chromebook program across 7 schools and 9,000 devices, cutting device loss by 68% and saving over $200,000 annually with centralized management.

Managing a 1:1 Chromebook program is difficult enough at a single school. Multiply that by seven buildings, 9,000 students, and a lean IT team, and you begin to understand the challenge facing Southeast Delco School District in suburban Philadelphia. This **school district chromebook management case study** documents how the district moved from fragmented spreadsheets and reactive firefighting to a unified, data-driven device management operation that serves as a model for mid-size districts across the region.

Southeast Delco's story is not about a massive budget or a large technology staff. It is about a district that recognized its existing approach was unsustainable and made a deliberate investment in the tools and processes needed to manage devices at scale.

District Profile: Southeast Delco School District

Southeast Delco School District serves approximately 9,200 students across seven schools in the suburban Philadelphia community of Delco, Pennsylvania. The district includes four elementary schools, two middle schools, and one high school, spanning a diverse suburban community with a mix of socioeconomic backgrounds. According to **NCES public school data**, districts of this size represent the most common district configuration in the United States, making Southeast Delco's challenges and solutions broadly applicable.

- **Total students:** 9,200

- **Total Chromebooks:** 9,400 (including spare pool)
- **Schools:** 7 buildings
- **IT staff:** 1 IT director, 2 full-time technicians, 1 part-time help desk coordinator
- **Deployment model:** 1:1 take-home for grades 3 through 12, shared carts for grades K through 2
- **Annual technology budget:** $1.2 million (devices, infrastructure, staffing, and licensing)

The district launched its 1:1 program in 2021, initially funded through a combination of ESSER funds and the regular technology budget. By the second year, the program was experiencing significant growing pains that threatened its long-term viability. **CoSN research on 1:1 program sustainability** shows that districts without centralized management infrastructure commonly hit these same inflection points in years two and three.

The Challenge: Seven Schools, Seven Systems, Zero Visibility

When Director of Technology Mike Petersen took stock of the district's device management situation at the end of year one, the picture was sobering. Each of the seven buildings had developed its own approach to tracking devices, and none of them communicated with each other.

The Spreadsheet Problem

Four buildings used Google Sheets for device tracking. Two used Excel files stored on a shared drive. The high school used a combination of a Google Form for check-out and a spreadsheet that a secretary updated manually. None of these systems captured the same data fields, and none of them were connected to the Google Admin console or the student information system.

"We had seven different versions of the truth," Petersen recalls. "When the superintendent asked me how many devices we had deployed and how many were missing, I had to spend three days reconciling spreadsheets from every building before I could give him an answer. And I was never confident the answer was accurate."

The Visibility Gap

Without centralized tracking, the district had no way to answer basic operational questions in real time:

- How many devices are currently assigned vs. unassigned across the district?
- Which building has the highest damage rate, and is it getting better or worse?
- How many devices are in repair right now, and what is the average turnaround time?

- How many devices have not connected to the network in the past 30 days?
- What is our total cost of repairs year to date?

The answers to all of these questions required manual data gathering from multiple sources, a process that was so labor-intensive it was only done during major inventory audits.

The Impact on Students and Staff

The lack of a cohesive system had tangible consequences beyond administrative inconvenience:

- **Device loss rate:** The district's end-of-year audit revealed a 6.8% loss rate, translating to roughly 640 devices and over $192,000 in replacement costs. **EdTech Magazine's analysis of district device programs** puts average loss rates for unmanaged 1:1 programs in the 5-8% range, making Southeast Delco's experience unfortunately typical.
- **Repair backlog:** Without a centralized repair queue, damaged devices piled up in each building's front office. Average repair turnaround was 22 days, and some devices sat for over two months.
- **Student downtime:** On any given day, an estimated 4.5% of students in grades 3 through 12 did not have a working device, creating instructional gaps and equity concerns.
- **IT staff burnout:** The two full-time technicians spent roughly 40% of their time on administrative tasks like updating spreadsheets, reconciling records, and responding to status inquiries from principals, time that should have been spent on repairs and support.

The Decision: Why Southeast Delco Chose Centralized Management

The tipping point came during a school board meeting where Petersen presented the year-one audit results. Board members were alarmed by the loss rate and repair costs, and they asked a pointed question: "What would it cost to fix this, and what would it save us?"

Petersen's team evaluated three options: building a custom tracking system using Google Apps Script, adopting a generic IT asset management tool, and implementing a purpose-built K-12 device management platform. After a four-week evaluation, the district selected UserAuthGuard based on several factors:

1. **Native Google Workspace integration:** The platform synced directly with the district's Google Admin console, eliminating the need for duplicate data entry across systems.
2. **Multi-school architecture:** The **multi-school dashboard** was designed for exactly the kind of cross-building visibility the district lacked.

3. **K-12 workflow focus:** Unlike generic asset management tools, UserAuthGuard's workflows were built around school-specific processes like seasonal deployment, end-of-year collection, and student-to-device assignment.
4. **Repair queue integration:** The ability to track repairs alongside device assignments in a single platform meant the district would not need a separate ticketing system for hardware issues.

Implementation: A Phased Approach Over One Summer

With only eight weeks between the end of school in June and the start of the new year in August, Petersen's team needed an implementation plan that was both thorough and realistic for a four-person IT department.

Phase 1: Data Migration and Cleanup (Weeks 1 through 3)

The first step was consolidating the seven disparate tracking systems into a single database. This was more complex than expected because each building's spreadsheet used different conventions for recording serial numbers, asset tags, and student assignments.

- The team exported all seven spreadsheets and reconciled them against the Google Admin console's device inventory.
- They discovered 340 devices that appeared in spreadsheets but were not enrolled in Google Admin, and 215 devices enrolled in Google Admin that did not appear in any spreadsheet.
- After physical verification, 180 of the "missing" devices were located in storage closets, repair bins, and one memorable case where 30 Chromebooks were stacked in a janitor's supply room.
- The remaining unlocatable devices were flagged as lost and factored into the year-one loss rate calculation.

Phase 2: Platform Configuration (Weeks 3 through 5)

With clean data in hand, the team configured UserAuthGuard to mirror the district's organizational structure:

- Seven schools were set up as separate entities with building-level administrators.
- Device pools were configured for each building, including assigned devices, shared carts, spares, and repair inventory.
- Repair workflows were standardized across all buildings with consistent intake processes, priority levels, and escalation rules.
- Automated alerts were configured for devices inactive for 7, 14, and 30 days.

- The Google Admin console integration was established, enabling bi-directional sync of device records, OU placement, and enrollment status.

Phase 3: Staff Training and Rollout (Weeks 5 through 8)

Training was the most critical phase. The best platform in the world is useless if the people who need to use it daily do not understand it.

- Building secretaries received two-hour training sessions on the check-in/check-out workflow, since they were the primary point of contact for device issues at most buildings.
- The two technicians received in-depth training on the repair queue, parts inventory tracking, and reporting tools.
- Building principals received 30-minute overviews focused on the dashboards and reports they would use to monitor their building's device health.
- Quick-reference guides were created for each role and posted in building offices.

Key Results: Year-Over-Year Impact

The most meaningful measure of success in this **school district chromebook management case study** is the year-over-year comparison between the district's pre-implementation baseline and the two years following the rollout.

Device Loss Reduction

- **Year 1 (pre-implementation):** 6.8% annual loss rate (640 devices, approximately $192,000)
- **Year 2 (first year with UserAuthGuard):** 3.4% annual loss rate (320 devices, approximately $96,000)
- **Year 3 (second year with UserAuthGuard):** 2.2% annual loss rate (207 devices, approximately $62,000)

The 68% reduction in device loss over two years represents cumulative savings of approximately $226,000 in avoided replacement costs.

Repair Turnaround Improvement

- **Year 1:** 22-day average repair turnaround, with some devices waiting over 60 days
- **Year 2:** 6.5-day average turnaround
- **Year 3:** 3.8-day average turnaround

The improvement came from three factors: centralized repair queue visibility, parts inventory tracking that prevented stockouts, and standardized workflows that eliminated the guesswork from the repair process.

IT Staff Time Savings

The two full-time technicians estimated they reclaimed approximately 15 hours per week combined that had previously been spent on manual record-keeping, status inquiries, and data reconciliation. That time was redirected to proactive maintenance, professional development, and building stronger relationships with teachers and building staff.

Student Device Availability

- **Year 1:** 4.5% of students without a working device on any given day
- **Year 2:** 1.8% of students without a working device
- **Year 3:** 0.9% of students without a working device

This improvement was driven by faster repairs, better spare pool management, and the loaner device workflow that ensured students received a replacement within 24 hours of reporting a problem.

Features That Made the Biggest Difference

When asked which specific capabilities had the most impact on the district's results, Petersen and his team consistently highlighted four areas.

Multi-School Dashboards

The **multi-school dashboard** gave Petersen something he had never had before: a single view of the entire district's device health. He could see at a glance which buildings had repair backlogs, which had spare shortages, and which had the highest damage rates. This visibility enabled proactive intervention rather than reactive firefighting.

"Before, I found out about problems when a principal called me or when a parent complained to the school board," Petersen says. "Now I see issues developing before they become crises. If I notice a building's damage rate spiking, I can investigate before it gets out of hand."

Automated Inactivity Alerts

The automated alerts for inactive devices were the single biggest factor in reducing the loss rate. In the first semester after implementation, the district recovered 89 devices that would have gone

undetected until the end-of-year audit. Most were found in students' homes, forgotten in closets or backpacks.

Centralized Repair Queue

Moving from seven informal "drop it at the front office" repair processes to a single, workflow-driven repair queue transformed the technicians' ability to manage their workload. They could prioritize repairs by age, severity, and warranty status, and principals could check on their building's repair status without calling or emailing the IT office.

Compliance and Board Reporting

Generating reports for the school board, which had previously required days of manual data assembly, became a matter of selecting a date range and clicking export. The transparency that accurate, timely reporting provided was critical to maintaining board support for the 1:1 program.

Lessons Learned

Southeast Delco's experience offers several lessons for other mid-size districts considering a similar transformation.

Start with Clean Data

The data migration and cleanup phase was the most time-consuming part of the implementation. Petersen's advice: "Do not assume your current records are accurate. Plan for at least two weeks of reconciliation and physical verification. Every device you locate during cleanup is a device you do not have to replace."

Standardize Before You Automate

Before configuring the platform, the team developed standardized processes for device check-out, damage reporting, repair intake, and end-of-year collection. Automating inconsistent processes just creates faster inconsistency.

Invest in Training for Non-IT Staff

Building secretaries and front-office staff are the front line of device management in most schools. Training them thoroughly on the check-in/check-out workflow paid dividends far beyond what additional technician training would have achieved.

Use Data to Drive Conversations, Not Blame

When the dashboards revealed that one elementary school had a damage rate three times higher than the district average, the natural instinct was to ask what that building was doing wrong. Instead, Petersen used the data to start a constructive conversation with the principal that identified the root cause: inadequate charging and storage infrastructure in several classrooms. A modest investment in charging carts and protective cases brought that building's damage rate in line with the district average within one semester.

Plan for Ongoing Refinement

The system is not set-and-forget. Southeast Delco reviews its alert thresholds, workflow configurations, and reporting templates quarterly. Each review produces small adjustments that compound into significant improvements over time.

The Financial Picture

For districts evaluating the return on investment of a centralized device management platform, Southeast Delco's numbers tell a compelling story:

- **Annual platform and licensing cost:** Approximately $18,000
- **Year 2 savings from reduced device loss:** Approximately $96,000
- **Year 3 savings from reduced device loss:** Approximately $130,000
- **IT staff time savings (estimated value):** Approximately $35,000 per year
- **Two-year return on investment:** Over 600%

These figures do not account for the harder-to-quantify benefits: improved student device availability, reduced instructional disruption, better board confidence in the technology program, and the reduction in stress on the IT team.

What Southeast Delco Is Planning Next

With the core device management operation running smoothly, Petersen's team is now focused on extending the platform's capabilities:

- **Parent portal integration:** Giving parents direct visibility into their child's device status, upcoming collection dates, and any outstanding fees.
- **Predictive maintenance:** Using repair history data to identify devices that are likely to fail based on age, model, and repair frequency, enabling proactive replacement before failure disrupts a student's learning.

- **Expanded analytics:** Deeper analysis of device utilization data to inform curriculum decisions and professional development investments.

See How UserAuthGuard Can Work for Your District

Southeast Delco's results are achievable for any mid-size district willing to invest in the right tools and processes. Whether you manage 2,000 devices or 20,000, the fundamentals are the same: centralized data, standardized workflows, automated accountability, and real-time visibility. Read more about our multi-building management capabilities on the **Southeast Delco case study page**, or explore the **multi-school dashboard features** that made the difference.

Schedule a demo to see how UserAuthGuard can help your district reduce device loss, streamline repairs, and build a 1:1 program that scales.