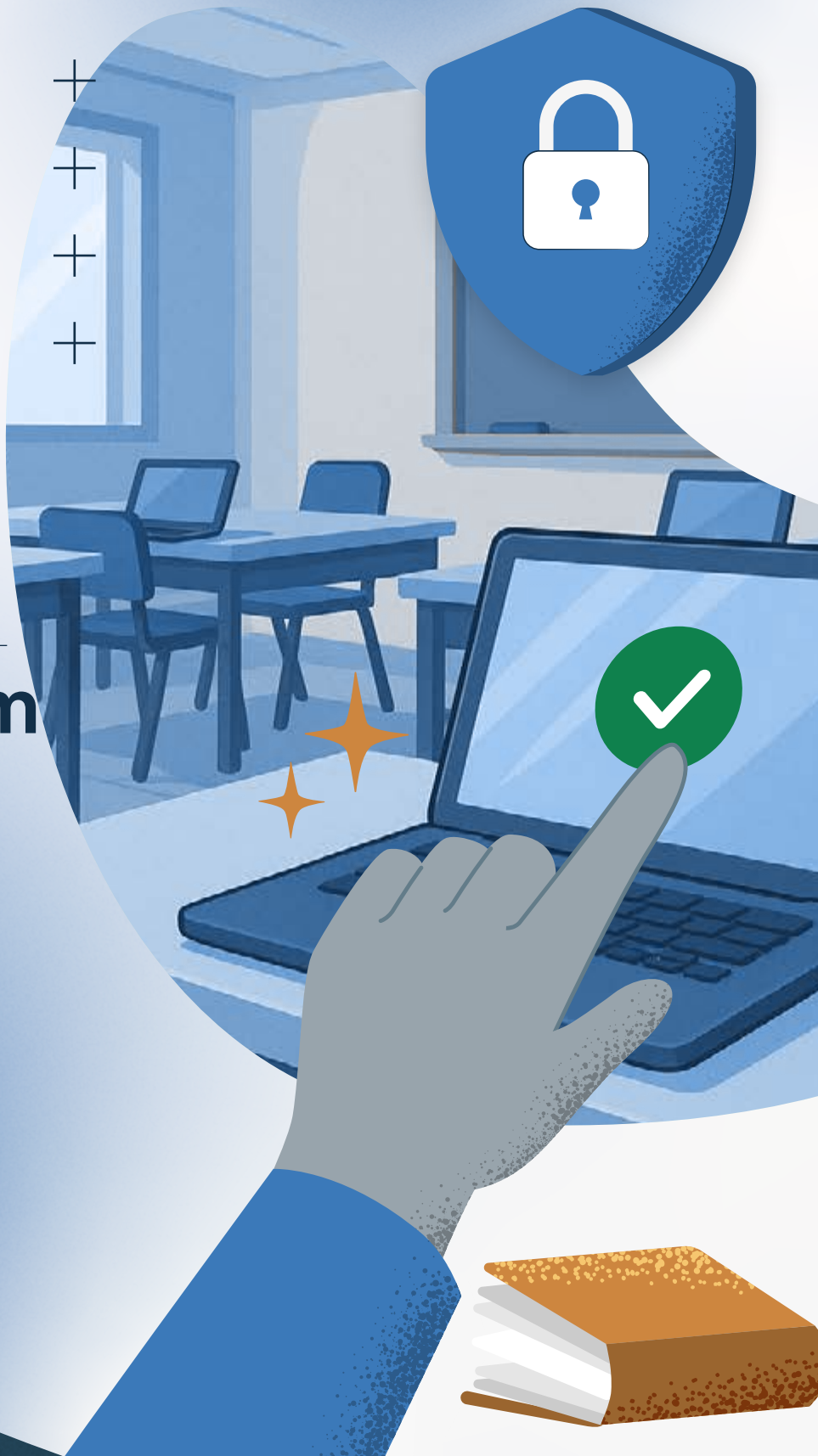
prey

How to stop your next school year 1:1

program from becoming a device chaos



Prey Inc.

Another school year is coming fast, and if you manage a 1:1 program, you know what that means: late summer returns, ghosted devices, outdated policies, and a flood of tech tickets before homeroom even starts. Sound familiar?

Let's break the cycle. With the right planning (and tools), your school can roll out student devices without the chaos. Here's how to get ahead of it.

Start with a real device audit (not a spreadsheet guessing game)

If you're relying on last year's Excel file to figure out what you actually have in your fleet... stop. Step one is a real-world device audit:

- **Check what was returned, what's usable, what's missing:** Get a real count—inventory reports don't mean much if 30% of your fleet didn't come back after summer.
- **Identify what needs repairs, replacement, or reconfiguration:** Look for hardware issues, aging batteries, or software problems that need to be resolved before reassigning.
- **Use a device management tool like Prey to track current status, assigned student and last known locations:** Instead of guessing, let the system show you where devices are, who had them last, and their current condition.

Go beyond the numbers. A proper audit helps you prioritize which devices can be recycled, which ones need to be replaced, and where unexpected gaps might appear due to transfers, theft, or under-the-radar damage.

Set policies students (and staff) will actually follow

Acceptable Use Policies shouldn't live in a PDF graveyard. Review and refresh policies so they're:

- **Simple and clear for students and parents**
  Use plain language, avoid legalese, and make it obvious what is—and isn't—okay.
- **Enforceable with your MDM or device tracking tool**
  If you say a device shouldn't leave school property, your tools should help you detect and respond when it does.
- **Aligned with FERPA/CIPA and your school's risk tolerance**
  Make sure your policies cover both student safety and regulatory compliance to protect your institution.

When policies are hard to find or understand, they're easy to ignore. Work with your legal or compliance team to ensure policies reflect how devices are used in the real world, not just the ideal one. Consider adding visual explainers or onboarding videos to increase understanding.

Bonus: bake in automated actions for lost or stolen devices. If a laptop leaves a geofenced area, Prey can alert you or lock it automatically—removing the guesswork and shortening your incident response time.

Don’t distribute until you’re secure

Too many schools rush device handouts before locking down basic protections. Before devices hit student hands:

- **Factory reset and wipe old profiles:** Ensure no lingering data or rogue profiles compromise the new user or school network.
- **Install security apps and configure firewalls:** Baseline security setup keeps malware and unauthorized access at bay from day one.
- **Activate Prey to monitor and remotely lock/wipe if needed:** Enable tracking, alerts, and incident response so you can act fast when devices go missing.
- **Set up basic geofences (school, home, off-limits zones):** Automate notifications and reactions when devices move outside approved zones.

This isn’t just about protecting hardware. You’re also safeguarding sensitive student data and avoiding potential FERPA violations. Build a pre-distribution checklist and test a few units to confirm they meet your district’s security standards. If something goes wrong later, you’ll know you shipped a secured device.

Pilot your rollout before going school-wide

Start small. Give a limited group of teachers or a single grade early access and treat them like beta testers. This helps you:

- **Spot compatibility or access issues before full deployment**
  Catch technical problems with apps, permissions, or connectivity early.
- **Build internal champions who can support peers**
  Your early users can become the go-to troubleshooters in their grade or department.
- **Adjust logistics based on real feedback**
  Use what you learn to refine distribution flow, support processes, and comms.

Pilots help reduce risk and generate insights. Use a quick feedback form or host a debrief with your pilot users to catch problems early. Even a one-week dry run can prevent hundreds of support tickets down the line. And don't forget to document your wins—those internal champions can advocate for the program district-wide.

Automate what you can, audit what matters

Manual tracking = burnout. Automate wherever possible:

- **Use Prey to schedule loan periods and get alerts on overdue devices:** Don't rely on memory or manual check-ins—set it and forget it with automated tracking.
- **Set rules to auto-tag or lock devices that don't check in:** Create workflows that act when devices behave unexpectedly—like going dark for too long.
- **Run regular reports on inventory, compliance, and incidents:** Use data to stay on top of device health and spot trends before they become problems.

Not every issue deserves a help desk ticket. Build workflows where routine triggers (like overdue returns or geofence breaches) are automatically handled, freeing up your team to focus on training, support, and long-term strategy. Bonus: automated audit trails also come in handy during board meetings or compliance reviews.

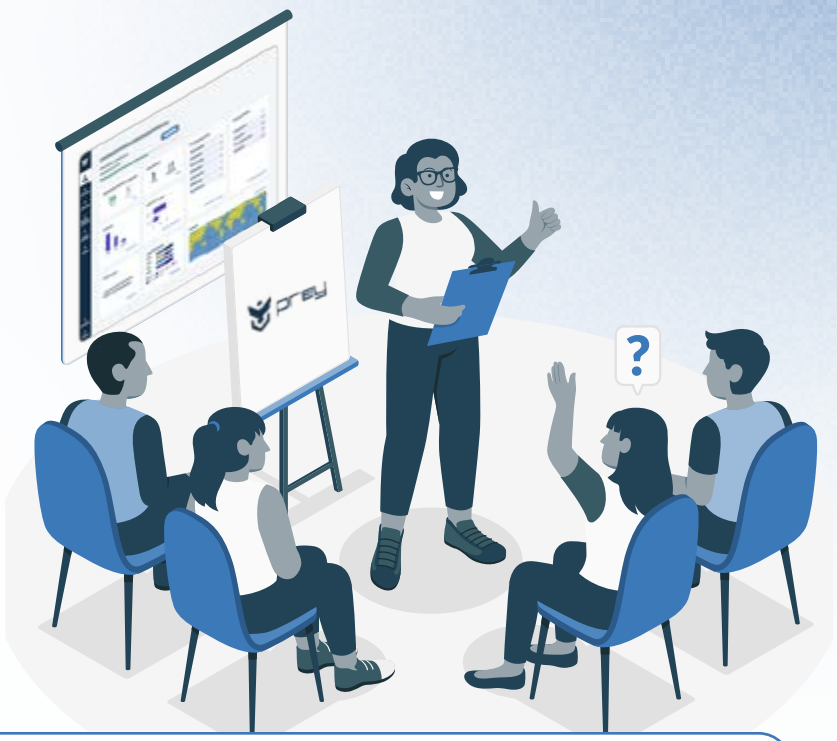
Have a documented incident response plan

When a device is lost, stolen, or compromised, your team shouldn't be scrambling. Build a response playbook.

- **Define roles and escalation procedures**
  Clarify who does what when a device goes missing or is involved in a breach.
- **Preconfigure Prey to lock, wipe, and track based on triggers**
  Set rules ahead of time so you can act within minutes—not days.
- **Inform students and parents about how incidents are handled**
  Transparency builds trust and reduces panic when something goes wrong.

This keeps your response fast, consistent, and aligned with privacy obligations.

Build digital literacy and onboarding into your rollout



You can't assume everyone knows how to use devices—or protect themselves online. Onboarding is key.

- **Offer cybersecurity basics to students**
  Cover phishing, safe browsing, password hygiene, and how to report sketchy activity.
- **Train staff to handle common issues and use Prey tools:** Empower support staff with quick how-tos and escalation guidance.
- **Use videos, quizzes, or student-friendly infographics:** Meet users where they are and make learning about security less boring.

This not only prevents issues—it creates a culture of responsibility and awareness.

Plan your end-of-year recovery before the first day

Thinking ahead isn't just smart—it's necessary. A successful device return process starts before the first device is handed out.

- **Set return expectations and dates at the time of distribution**
  Don't leave it open-ended—build a return window into your loan policy.
- **Use Prey to automate return reminders and overdue alerts**
  Schedule reminders a few weeks and days before devices are due back.
- **Maintain ongoing records to avoid device ghosting**
  Update assignments as students transfer or leave mid-year to reduce year-end surprises.

With proactive planning, you'll close the year with fewer lost devices and less stress.

Your tech strategy deserves better than survival mode

Every year doesn't have to start in a panic. By combining smart planning with the right tools, you can roll out devices with less stress, more security, and total visibility.

Need a deeper checklist or help planning your rollout?

Download the Back-to-School Device Checklist or
Talk to us about your 1:1 strategy

About Prey

Prey is a cross-platform **Device Tracking & Security** tool to stay in control of remote assets. It's a service that protects over 8 million devices and their data every day, all around the world.

Prey started in 2009 as a small tech company with a sole purpose: helping people keep track of their devices. 15 years later, our service evolved into a trusted multi-tool for both people and businesses. We are experts at tracking, protecting and managing your work and play tech tools. And a proud team of people willing to support you.

Prey for: People | Businesses | Schools

Prey Inc. ©
548 Market St. #30152
San Francisco, CA 94104
USA