Simplifying Device Management in Education Via Managed Desktop as a Service

COX BUSINESS® | Cloud Solutions

Introduction

Over the last 25 years, education has shifted from being purely classroom- and textbook-based to one where teachers are supported by a wealth of technology. For the past year or so, the learning experience has been almost entirely virtual. Without devices – whether desktops, tablets, or laptops – teaching would have been impossible.

Now that people are returning to the classroom, devices will play an increasingly important role in the educational process.

Schools will have to ensure that every student is armed with the right device, laptops or Chromebooks in most cases.

That entails the procurement, management, repair, and disposal or repurposing of anywhere from hundreds to thousands of laptops each year. Yet schools are in the business of education, not device management. Teachers and administrators want to maximize the time they spend fulfilling their educational purposes. Every minute spent in laptop management and troubleshooting detracts from the achievement of learning objectives.

Unfortunately, some schools have become bogged down in the problems of laptop ownership. Technology budgets have spiraled out of control and become a major drain on already tight, limited budgets. Entire classrooms have become cluttered with broken or obsolete devices. Large teams of IT specialists have had to be hired to support classroom technology.

The underlying problems are twofold:

1. Device management is not the province of educators and challenging for small district IT teams to keep on top of.

2. Procurement accounts for only a fifth of the overall lifecycle cost of a device. About 80% is absorbed in installing software and updates, management devices, repair, security, help desk, and device disposal.[1]

This guide has been produced to assist school systems in addressing the device management challenge more efficiently. Inside, you will learn how to:

• Simplify device management

• Reduce lifecycle costs: This can be accomplished by lowering the total cost of ownership (TCO) for devices across their lifespan by optimizing processes for selection, acquisition, provisioning, deployment, and disposal

• Heighten the protection and online security of students

• Boost student satisfaction and productivity

• Reduce the IT burden connected with devices, enabling the IT team to focus on strategic aspects of educational technology

Managed Device as a Service (MDaaS) is emerging as the solution to these challenges. MDaaS for Education from Cox Business provides a choice of devices, core applications, device maintenance, and even replacement all for one low cost for students, faculty, and staff.

[1] The Fintech Times, Uncovering the Hidden Costs of Ageing IT Equipment, 2019, https://thefintechtimes.com/costs-of-ageing-it-equipment/

The Problems of Device Management

Many schools buy devices for their students and try to manage them internally. Often, they are soon overwhelmed by the time, resources, and cost of management those devices through their lifecycle. Studies show that the bulk of device costs are tied up AFTER device purchase.

Device purchasing generally receives far more attention than overall device lifecycle costs. But the surprising fact is that most lifetime costs are tied up in managing and maintaining of devices. That's why too narrow a focus on hardware purchasing can lead to expensive errors.

The purchase price for devices averages about 20% of their overall TCO. Additional costs over their lifetime dwarf the spending on hardware alone. The rest of the money is consumed by device management and support.[1]

These costs rise even higher as the equipment ages and as the performance and reliability of the device decreases. Decisions to delay device replacement, therefore, may conserve cash over the short term. However, IT support costs rise steadily, and student satisfaction and productivity rates can decline.

Here is an actual example of a system of 35 schools and 10,000 seats. Each student was provided with a Chromebook. Every year 2,500 seats changed. The district tried valiantly to manage these devices. Very soon, it had devoted three large classrooms to device management. Each room had rows of shelving filled to the ceiling with broken devices gathering dust or Chromebooks in need of service – software updates, new images, better security, etc. Eight personnel were kept busy throughout the school year keeping up with the administration and servicing of devices for students. Yet despite all this attention, students gave the school district low marks for device quality and user satisfaction.

Far from being a vital function of modern schooling then, device management has become a major distraction to the overall mission of educating students and the precious little time they have to be dealing with such tasks. The reality is that schools should not be in the business of managing devices. The students of today are the building blocks of a new tomorrow. They need to be supported by an education system devoted to the relay of the vital skills and knowledge needed in a functioning society.

Consider the many duties involved:

Device procurement: Every year, a school needs to have a sufficient number of devices on hand for the incoming student body. If they have to acquire new devices, that entails engagement with suppliers, negotiating the best bulk discounts, budgeting for the funds, placing the orders, receiving the goods, unpacking the equipment, and disposing of the boxes and packing materials.

Configuration and deployment: Once received, each device must have additional software installed, drivers updated, and must be logged as a device operating on the network before being assigned to a student. They must be configured correctly with the appropriate features, learning and security applications, and deployed efficiently to the student body in accordance with school policy.

Training and adoption: Although today's students are generally technology savvy, there are still some that need training on how to use devices and applications. And others will have questions about the peculiarities of Chromebooks, trouble with network access, and problems in getting the most out of certain applications. This is especially true of elementary school students.

Device maintenance: Devices need constant attention. Software and hardware issues must be resolved, updates and patches installed, warranty issues dealt with, and network connectivity maintained. This necessitates a manned help desk that can respond to student needs effectively and in a timely manner. IT must be attentive to student requests to ensure they become productive.

Device repairs: In the hands of a large student body, accidents and damage are inevitable and occur with regularity. Personnel must exist with the requisite skills to address problems such as broken screens and keyboards, faulty hard drives, and the many other issues that will arise.

Device disposal: Each year, there will be laptops and Chromebooks that are either too badly damaged to have further value or have reached their end of life and need replacement. This can add up to hundreds or even thousands of devices annually. Let's return to our 10,000-student school district example. If 2,500 new students enter the system each year, and devices have a four-year lifespan, that's at least 2,500 new devices needed each year – more when you factor in broken and irreparable equipment. That's a lot of devices to dispose of. Each one needs to have all its data wiped, and then its drives rendered utterly unreadable. This alone can take several hours per device. Once done, all equipment must be transported to a disposal facility.

But with the right processes in place for the management of devices from the beginning of their lifecycle to the end, schools can lower IT costs and boost educational outcomes.

Device Management Distracts from Educational Duties

Schools need devices to facilitate education. But priorities are clear: a focus on education is paramount, not looking after devices. Yet teachers are often forced to act as defacto IT support techs. Since device management is not the core competency of any school, it is no wonder that many school districts struggle with the function.

Even when they can afford skilled, well-manned IT departments, device management eats up valuable time that should be spent on driving educational objectives. In many cases, the establishment of a school's IT department was meant to enhance the learning experience by implementing the latest educational applications and platforms and find ways to improve the learning experience for the student. Yet these noble objectives often find themselves derailed by the burden of keeping devices operating and fielding an endless cacophony of help desk calls from distraught students about the latest problem.

Attempting to cope with device ownership and management internally can result in a series of unforeseen consequences:

- Devouring the IT budget with little money or resources left over for strategic IT priorities

- Long delays in servicing devices and returning them to students

- Emergency requests for the procurement of loaner devices due to mounting repair and service backlogs

- Endless security concerns due to out-of-date patches and updates, as well as risky student behavior

- Vital educational projects taking far too long to complete due to IT resources spending time on other duties

- Poor student satisfaction ratings on devices

Yet the fact remains that students must be properly equipped for 21st century learning. They must be provided with modern devices that are secure, issue-free, and procured or managed correctly in order to lower TCO over their lifespan.

By reevaluating the way to obtain, manage, and service student devices, schools have an opportunity to take advantage of advances in cloud infrastructure, artificial intelligence, and digital transformation while enhancing cybersecurity to protect the devices, their network environments, staff, and perhaps most importantly the students.

An end-to-end, managed approach to student devices can help to:

- Reduced IT costs
- Optimized IT processes
- Increased productivity
- Greater employee satisfaction

School Security and Safety

The following issues related to school security and safety are on the increase in society. These issues are on the increase in society. According to the [Annual Report: 2020 Research on Children and Technology](#)[2], an analysis of more than 2.1 billion student messages across texts, email, YouTube, and more than 30 additional apps and social media platforms revealed some shocking results:

- **Violence:** 88.5% of tweens and 94.1% of teens expressed or experienced violent subject matter/thoughts.

- **Mental Health:** 45.5% of tweens and 66.3% of teens engaged in conversations about depression.

- **Bullying:** 76.7% of tweens and 82.0% of teens experienced bullying as a bully, victim, or witness.

- **Drugs/Alcohol:** 78.0% of tweens and 91.1% of teens engaged in conversations surrounding drugs or alcohol.

- **Self-Harm/Suicide:** 41.4% of tweens and 66.6% of teens were involved in a self-harm or suicidal situation.

- **Sexual Content:** 70.9% of tweens and 87.9% of teens encountered nudity or content of a sexual nature.

If students are issued with devices, they will use them for more than classroom study and homework. They will also be used for social media, web, email, and texting. When any device strategy is being developed for schools, therefore, it must incorporate the aspect of risk reduction.

[2] Bark, Annual Report: 2020 Research on Children and Annual Report: 2020 Research on Children and Technology, 2020, https://www.bark.us/annual-report

And most administrators, teachers, IT staff and even parents aren't even aware that one of the most common ways that students interact is not just through social media, but through the creation of quasi-chat rooms built through sharing of documents like Microsoft Word and OneNote, or Google Docs. This is yet another front for considering how to help protect students from cyber predators, given possible exposure risks inherent in Google Workspace, but even just from their own behaviors.

Security is another key factor. Malware and ransomware incidents have increased dramatically. Cybersecurity firm CrowdStrike found more intrusion attempts in the first half of 2020 than in all of 2019.[3] The company's threat hunting team blocked more than 40,000 potential intrusions compared to 35,000 in the previous 12 months. Such issues are only made worse by the presence of old laptops and Chromebooks running unsupported applications on obsolete operating systems, or just those that have known security holes.

[3] IntelligentCISO, New CrowdStrike report reveals more cyberattacks in the first half of 2020 than 2019, 2020, https://www. intelligentciso.com/2020/09/17/new-crowdstrike-report-reveals-more-cyberattacks-in-the-first-half-of-2020-than-2019/

With malware incursions and phishing attempts continuing to grow in number and in their level of sophistication, student should not be exposed to risk by forcing them to operate with outdated hardware. Failure to do so will prove expensive, both in terms of time and budget.

School networks are a frequent target for cybercriminals, given their resource constraints, possible lack of security expertise and vulnerable, unsavvy user base.[4] Around 60 U.S. school districts suffered ransomware attacks in 2020. In many cases, the attackers managed to extract and publish staff and student data. It got so bad that the FBI issued an alert about the increased incidence of ransomware attacks on schools.[5]

It's easy to see why cybercriminals enjoy so much success against educational targets. With thousands of devices in student hands, each one represents a possible avenue of incursion. All it takes is one lax user and the bad actors can gain unauthorized access to the network. Once inside, they can install malware, exfiltrate data, encrypt school systems to lock out users, and hold the organization to ransom. Typically, they threaten to make stolen data public if a sum of money is not paid.

Recent ransomware victims include Haverhill Public Schools in Massachusetts, Park Hill School District in Missouri, Buffalo (N.Y.) Public Schools, Clark County in Nevada, Fairfax County in Virginia, Toledo in Ohio, and Broward County Public Schools district in Florida. The latter case against the nation's sixth largest school district demanded a $40 million ransom. When this demand was refused, tens of thousands of sensitive school files were published on the dark web.

Security, then, is no small matter. But risk reduction and security place additional constraints on an already overstretched school administration and IT department. Fortunately, solutions are available for education that bundle device management with protection of the student body and the school network via Bark for Schools software and services.

Trusted by over 2,800 districts in the U.S., this powerful student protection software uses artificial intelligence (AI) to scan websites, email, and other media for potentially dangerous behavior or traffic. This includes scanning student Google Workspace and Microsoft 365 accounts (including emails, chats, and files) for potential issues like threats of violence, self-harm, cyberbullying, and more. It offers administrators and the parents of students insights and timely alerts so they can help keep students safe. The solution is CIPA-compliant. Perhaps most importantly, Bark for Schools layers in live, highly trained experts who monitor severe alerts and personally notify concerned parties families and administers of urgent concerns.

[4] Data Breach Today, Ransomware Attacks on Schools: The Latest Developments, 2021, https://www.databreachtoday.com/ransomware-attacks-on-schools-latest-developments-a-16451

[5] Federal Bureau of Investigation, Cyber Division, Increase in PYSA Ransomware Targeting Education Institutions, 2021, https://www.ic3.gov/Media/News/2021/210316.pdf

What is MDaaS?

The good news is that the heavy load placed on IT by managing the devices of the student body can be eliminated by adopting the Managed Device as a Service.

MDaaS offers a way for educational institutions to reinvent virtual and classroom learning environments, improve communication between students and teachers, simplify administrative operations, and cut costs. Instead of purchasing the devices and being left with the problem of taking care of them for several years, the devices are leased and automatically replaced every three years. This ensures the student body is always provided with modern laptops and tablets.

A key differentiator among providers is the amount of care and understanding a provider invests in the customer's existing IT environment, needs of the organization, and how MDaaS fits in with ongoing strategic and educational initiatives.

The potential benefits of MDaaS include:

- Reduced infrastructure and and IT management costs.

- Reduction of costly capital expenditures (CapEx) by transferring budgeting to a low monthly, all-inclusive leasing fee per device.

- Regular device refresh and replacement costs are factored into the pricing.

- If a device is stolen or damaged, one replacement per lease term is included within the price.

Cox Business MDaaS for Education

Cox Business offers a way to empower faculty, students, and staff with reliable, flexible, secure and affordable managed devices via its all-inclusive MDaaS solution. With an extensive background supporting educational institutions, Cox Business MDaaS for Education allows students, faculty, and staff to work from virtually anywhere with a managed laptop, Chromebook, or tablet.

The simplicity and end-to-end support rolled into Cox Business MDaaS for Education provide a great many benefits:

- **Cost Efficiency:** Access hardware and support at one affordable, predictable monthly price.

- **Device Choice:** As well as Chromebooks, schools can select from a range of other laptops and tablets from HP, Samsung, and LG.

- **Hardware Replacement:** Avoid costly one-time hardware refresh costs when you renew your device at the end of the lease. Cox Business maintains a pool of spare devices to facilitate repairs, replacements, or warranty matters to ensure students always have reliable access to their devices.

- **Software Included:** Fully licensed Windows 10 software, and Microsoft 365 from Cox Business is available/optional with every device.

- **Microsoft Gold Partner:** Cox Business is trusted by Microsoft to deliver highly differentiated Microsoft 365 services.

- **Easily Scalable Solution:** Easily add new devices and services at any time without changing the per-device cost.

- **Full-Service Coverage:** Simplify device lifecycle management and IT hardware procurement, while easing other IT burdens that come with managing and supporting company devices.

- **Comprehensive 24/7 Support:** Cox Business provides a single point of contact and resolution for any issues relating to hardware, built-in software, performance, maintenance, repair, or replacement. Strong relationships with our technology partners allow us to rapidly resolve any issues on the first call.

- **Advance Replacement:** In the event your equipment needs to be fixed, we maintain a large pool of spare devices that allows advance replacement of devices within two business days. Warranty issues are also included as part of the service.

- **Bark for Schools:** This service scans emails, chats, and files for signs of serious issues, self-harm, threats of violence, cyberbullying, and sexual content, alerting parents and administrators of the threats. Highly trained school safety specialists review all severe alerts and personally notify the school of imminent issues. Terms and conditions apply.

- **Student Satisfaction:** Cox Business boasts a best-in-class 4.8 out of 5 customer satisfaction rating to ensure student device issues are promptly addressed.

Ready to get started?

Throughout the school year, many different device-related challenges arise. Cox Business certified engineers help keep all devices maintained, repaired, and operating to ensure students stay logged in, engaged, and learning. With this comprehensive MDaaS solution, there is no need to juggle the many tasks of a school-wide rollout of new devices such as coordinating third parties, staffing a help desk, supporting a pool of spares, or overseeing service and repair delivery.

Contact a Cox Business consultant today to find out if you qualify for educational discounts or other financial incentives that may be available courtesy of the CARES Act.

COX | **Cloud**
BUSINESS® | **Solutions**

For more information, visit
cox.com/business/cloud-services/mdaas.html