Stretch Budgets, Keep Control: The Case for Parent-Funded, School-Managed Devices

Overview

For many schools, it's time to procure new devices for the classroom. As schools wrestle with budgetary constraints, many are unsure how to proceed. **This paper examines the parent-funded, school-managed (PFSM) approach, which combines the cost benefits of traditional BYOD programs with the security and control of school-managed, supervised devices.** By choosing Apple and Jamf, devices become powerful learning tools that don't compromise security or privacy while empowering IT, teachers, students and parents.

Introduction

Today's schools face a growing challenge: delivering a high-caliber digital education while battling financial constraints and mounting threats to student data. Smoothly integrating technology into the classroom is a persistent challenge for schools, especially as funding ebbs and flows and devices evolve. COVID-19 demanded schools rethink the purpose of their tech strategy. Years later, in many ways, this hasn't changed, and **equitable device access remains a challenge**.

What You'll Learn

- How PFSM outperforms traditional BYOD
- How schools are shifting to parent-funded, school-managed device strategies
- How PFSM supports better security, learning outcomes and budget relief
- Real-world examples of PFSM adoption around the world
- A step-by-step checklist to set your school up for PFSM success
- How Apple and Jamf enable safe, seamless learning at school and at home

Schools are constantly adapting their technology strategy to improve learning and teaching. This can present some difficulties as they discover how to:

- **Acquire devices** that meet the needs of their learners
- **Enable students** of all backgrounds to have access to an internet-connected device
- **Fund** necessary device purchases
- **Ensure** the school's tech infrastructure can support these changes
- **Maintain** learning outcomes
- **Keep devices secure**, especially if they access school resources

Many schools received special funding in 2020, allowing them to purchase necessary devices and update their technology implementation. For many districts, this led to exciting new developments and a permanent shift in classroom learning. But as funds run out and devices reach their end of life, how can schools maintain the momentum of their digital transformations?

Schools around the world are searching for a solution, and it's not easy to find. There are a few options schools are exploring:

- **Government supported**: schools obtain devices with full government funding
- **Public-private partnerships**: government collaborates with other organizations to provide devices, possibly with parent funding
- **Loans or leasing programs**: schools loan or lease devices from industry providers
- **BYOD or parent funded, school managed**: parents/guardians provide devices for their own children, with or without government assistance

Need some context?
See how other districts and governments are addressing device procurement.

Uruguay's Plan Ceibal delivered laptops to all students in public schools.

The Austrian government allocated laptops or tablets for fifth and sixth grade students.

Parents in the UK can purchase or lease devices from industry partners that collaborate with their school.

Eligible schools in Maine, U.S. can finance devices with a tax-exempt municipal lease.

There's no "perfect solution", only complete strategies that fit your purpose. For government - or partnership-funded devices - the sheer amount of money that is required can be a hurdle, especially in communities that are already underfunded. **That's why many districts are exploring parent-funded device strategies**, where much of the cost is shouldered by students' families, who may purchase outright or lease a device. In some cases, assistance is offered to families who cannot afford a device.

With this approach, the devices belong to the student or their families — not the school. Students benefit from a familiar personal device, one they're more likely to care for and know how to use. Schools also avoid the burden of acquiring large quantities of devices, reducing potential delays.

This model is increasing in popularity. If this seems right for your school, there are important details to consider.

Parent-funded, school managed vs. traditional BYOD

You may already be familiar with BYOD — bring your own device — programs. And you may be wondering, how is a parent-funded, school managed (PFSM) program different from a BYOD one?

Put simply: both traditional BYOD and PFSM models involve parents purchasing a device for their student. However, with traditional BYOD, schools often get little or no control over devices. **In PFSM models, schools enroll these devices into their Mobile Device Management (MDM) solution.** So what does this mean in practice?

Configuration consistency

With traditional BYOD, device configurations can vary widely. Devices may not be set up for distraction-free learning and can create security risks.

PFSM devices are managed by the school, allowing for more consistent configuration. Students aren't disadvantaged by devices that, when shared with family, aren't optimized for learning. School IT ensures all students have the same access to apps, resources and tools.

Security implications

Traditional BYOD lacks standardized security controls. Devices access the school network and school resources, often containing private information — all at higher risk of a data breach.

PFSM improves security with centralized management and policy enforcement. With management, devices can be wiped if lost or stolen, passcode policies can be enforced and students can be protected from malicious websites and threats with network threat protection and content filtering.

Supervision and compliance

Traditional BYOD doesn't include device supervision, making it difficult or impossible to enforce school policies.

Since **PFSM devices** are enrolled in MDM, schools can enforce security and usage policies and monitor compliance.

Ownership and control

With traditional BYOD, devices are owned and fully controlled by the student or parent. The school has no control over how the device is used at home — including whether it can access harmful websites.

With PFSM, schools can enforce key security and content policies, even beyond school grounds. Students may have more freedom to access entertainment or other sites, but without putting themselves or their data at risk. And parents can pick up device supervision once their students are at home.

Why do schools adopt a PFSM model?

Budget constraints

School budgets vary widely depending on demographics, government sponsorship, country and more. For manyschools, it's impossible to provide devices for every student. A PFSM model shifts the cost to parents without sacrificing the control and security required for a successful device deployment.

Device management and supervision

With COVID-19, schools had to react quickly to provide devices to their now remote students. In many districts, this left open gaps that attackers exploited. Schools reacted to close the gaps, and management and supervision became clear requirements. Management and supervision make it possible to keep devices secure and ready for learning — otherwise, this is nearly impossible.

Flexibility for home use

Parents are spending their own money on their student's device. It's not reasonable to expect these devices will only be used by the student, at school and for learning. Schools need management solutions that allow for this without compromising privacy or security. Their MDM should be able to adapt to location and/or time for appropriate usage — so schools have control during class and parents take over after the final bell.

Did you know?

With Jamf Student and Jamf Parent apps, parents get supervision of their child's device after school hours. Parents get autonomy over the devices they purchased without introducing security risks for the school.

Benefits for PFSM models

If you've been keeping up with current events, you might have heard of two recent topics: cell phone bans and tariffs.

Cell phone bans are increasing in popularity around the world, as schools find them to be distracting and detriments to learning. Opinions on technology in schools can certainly be controversial. However, as UNESCO states in its **2023 GEM report**, technology should „focus on learning outcomes, not on digital inputs." In other words, technology implementation needs to both support and be supported by the curriculum.

This support isn't possible without schools having purview over these devices. Unsupervised devices mean practically unrestricted access to the internet, which can lead to distraction and potential harm. This can only hurt learning outcomes.

Tariffs are also affecting schools, especially in the U.S. Many schools launched 1-to-1 device deployments at the start of COVID-19, some relying on federal aid to purchase devices. As this aid runs out and devices reach their end-of-life, schools must figure out how to afford new devices.

PFSM deployments may offer a solution to these issues. How?

Data is secured and response times are reduced.

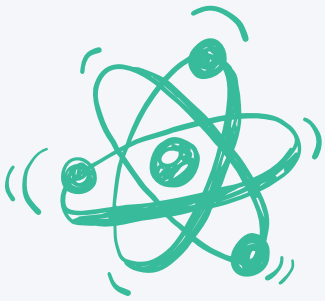
- Security protocols are consistent across all devices.
- IT admins know when devices fall out of compliance and can respond quickly.
- Schools can set and enforce compliance requirements on their devices.

Learning is more unified and equitable.

- Uniform devices configurations give all students equal access to resources.
- With fewer distractions, devices can be optimized for learning.
- Since IT can respond to issues quickly, there's less disruption to learning.

Schools save money.

- Schools face a reduced financial burden when purchasing devices — especially since they would have to repeat this process once devices reach end of life.
- Students can potentially have higher-quality devices, as they aren't limited by school budgets.
- The ability to secure these devices lowers the chance of data breaches, ransomware or other costly cyber events.



"In the longer term, districts might have to rethink their 1-to-1 computing-program plans altogether."

— **Eva Rodriguez Mendoza,**
Chief Information Technology Officer,
San Antonio schools

Checklist:
Set your school up for PFSM success

A successful PFSM implementation can be challenging. But there are actions you can take to increase the odds.

Parental engagement

Devices aren't cheap. When parents invest in tools that are then controlled by the school, they need to feel confident in that decision.

- **Explain what devices** will be used for and why they should be enrolled in your MDM
- **Be transparent** about data handling practices, ideally minimizing data collection
- **Empower parents** with control of their devices after they leave school grounds

Policy development

A good execution of PFSM requires careful planning and intention. That's part of what separates it from traditional BYOD.

- **Create or enforce** acceptable use policies (AUP) that reflect the shared responsibility between parents and schools
- **Decide** what restrictions devices should have and when they apply
- **Develop or implement** security controls

Device maintenance

Students can be rough on devices. Damaged devices can delay learning. And devices all require maintenance to ensure they're running at their best.

- **Establish a protocol** for repairs
- **Keep devices updated** with the latest software to ensure a consistent experience for all learners and to mitigate potential security risks
- **Develop a plan** to replace broken devices or have spare devices to loan out if needed

Understand your infrastructure

Your network may already support hundreds or thousands of devices. If not, some preparation may be required.

- **Understand** if networks can handle the load of many devices
- **Determine** the amount of bandwidth your infrastructure supports
- **Decide** how your network will be secured, especially if there are a large amount of new devices

The right PFSM implementation can improve learning outcomes.

As we've already mentioned, the device management you get with PFSM and not with traditional BYOD is significant. But the real power comes from what you can do *in the classroom.* With the right mobile device management (MDM) tools, your device implementation starts with IT and ends with empowered students and teachers.

Many schools choose iPad tablets for their students. It makes sense — iPad offers a host of educational apps, allows for device management and has an excellent feature set, including accessibility features. With Jamf, schools get device and classroom management tools made just for iPad.

Let's take a look at how Apple and Jamf set the foundation for great learning.

MDM powers consistent learning.

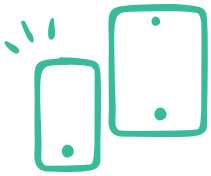
- **Device supervision**: With Jamf MDM and Apple's device supervision capabilities, IT can enforce configurations that standardize the learning experience across all devices.
- **App deployment at scale**: MDM makes large-scale app deployment simple — automatically deploy and manage essential education apps and tools with minimal (or no) downtime.
- **Restrictions and configuration profiles**: Restrictions disable apps or device features based on what IT or teachers deem appropriate. This makes devices powerful learning tools — not distractions.
- **Automated OS and app updates**: The latest updates mean the latest features and security patches. Keep devices secure and compatible with the latest learning tools, minimizing disruptions and support requests.
- **Dynamic grouping and smart targeting:** Not all learners have the same needs. Customize apps, settings and restrictions based on grade level, class or individual learning needs.

***How Jamf can help**: Configure your entire device fleet, deploy and update apps, enforce policies and more with Jamf School, MDM purpose-built for education.*

Security and safe browsing

- **Web threat prevention**: Protect students and school networks from phishing, malware and malicious sites with real-time threat detection.
- **Content filtering**: Customize access to web content based on school policies, grade levels, categories or even curriculum needs. This way, students can only access age-appropriate educational content. With on-device content filtering, students are protected from inappropriate content even if they aren't on school networks.
- **Remote lock/wipe**: Mitigate potential data loss by allowing IT to remotely lock or wipe a device if it is lost or stolen.
- **Security compliance**: Enforce passcodes, disk encryption, OS version controls and other device-level settings for devices that are secure and ready for learning.

***How Jamf can help**: Jamf Safe Internet offers content filtering and threat prevention wherever students are located. Jamf Protect keeps endpoints protected from malware and other harm while keeping IT informed with behavioral analytics.*



Classroom workflow support

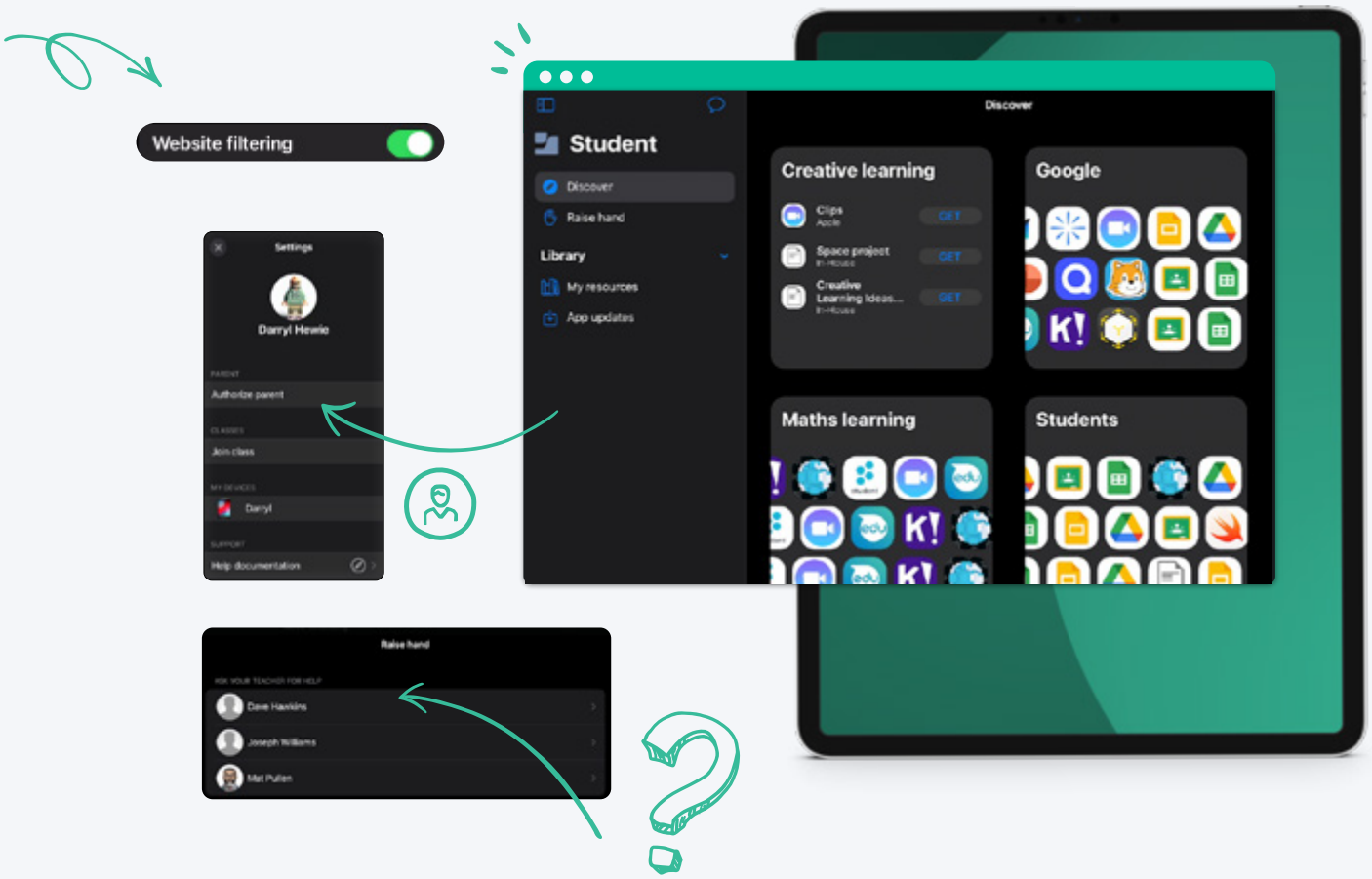
- **Real-time teacher tools**: Teachers can configure devices to match their lessons, lock devices to regain attention, communicate with students and monitor student screens.
- **Apple Classroom compatibility**: Apple Classroom is fully supported on supervised devices for digital classroom control.
- **App-based learning controls**: Lock devices into specific apps during tests or focus time.

***How Jamf can help**: Jamf Teacher lets teachers manage their student devices during lessons for classroom management and seamless integration with their teaching. Jamf Student guides learners and enables them to autonomously use their device — with guidance to keep them safe and on task.*

Home and school balance

- **Dual mode management**: Devices act as educational tools at school, then can be used for other purposes when students have free time.
- **Parental visibility and support**: Parents can control usage after school hours with app restrictions and screen time management.
- **Time-based policies**: Devices can be locked for educational use during specific times, preventing access to entertainment, social media and other websites. Change restrictions based on time, whether it's during a holiday, after school or even a specific lesson.

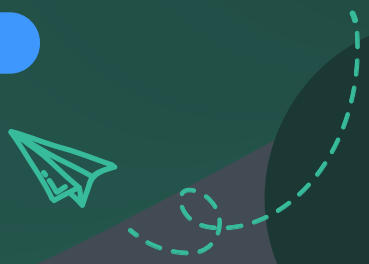
***How Jamf can help**: Jamf Parent gives guardians control over their students' device usage while respecting school configurations and security settings.*



Does a PFSM model seem right for your school?

See How IT Tools Can Impact Learning

Try Jamf



Key takeaways

- Many schools face challenges with device procurement.
- Traditional BYOD programs often leave gaps in security and learning.
- Device supervision and management is crucial to keep devices secure and consistent.
- A parent-funded, school-managed model alleviates a school's financial burden without compromising safety, security and learning outcomes.
- Jamf and Apple help schools go beyond device management and security by empowering IT, teachers, students and parents — everyone wins.

jamf