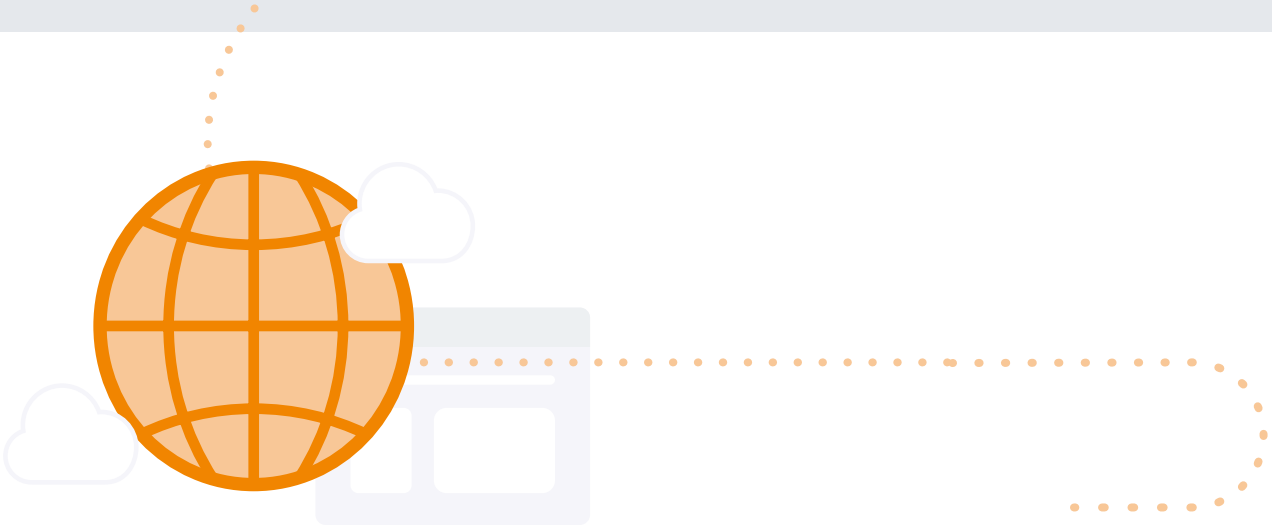
Content Filtering Essentials for K-12

jamf



Schools around the globe struggle to achieve the right internet balance: they want to give their students access to the incredible research and educational opportunities available on the web, and they also want to keep them safe from dangerous or inappropriate content as well as phishers and predators.

Kids are attempting to access inappropriate or dangerous content at school every day: In New Zealand, schools recently reported that they had blocked 399 million attempts to access inappropriate content in one month. [1]

And now that school-issued devices go home —outside of the school's firewall— schools need some mechanism in place that blocks access to inappropriate websites from their devices, no matter where students use them.

This means that schools must address student safety on many fronts. This guide is meant to help schools navigate this process.

In this guide, we'll discuss:

- What online content puts students at risk and why it's important to actively protect them
- The nuances and scenarios that warrant a flexible and customized approach to content filtering
- How to educate and empower your students on Digital Citizenship
- And how Jamf can help you

Why filter?

So many reasons.

Student protection

Legal restrictions on student online access varies from country to country, but they all fall into similar categories:

- Pornographic or obscene content
- Hate speech, violent or radicalizing sites
- Sites encouraging self harm, suicide or anorexia
- Phishing or predators
- Cyberbullying
- Removing distractions such as social media and games
- Gambling sites

According to the Worldwide Health Organization, suicide is the fourth leading cause of death globally among 15-19 year-olds.[2] And with anywhere between 47-60% (depending on age) of all school-aged students being cyberbullied,[3] protecting students from this type of online danger can literally save lives.

Student focus and productivity

While restricting social media access at school can prevent cyberbullying, it can also help keep students focused on school. This helps students to learn more and increase their productivity and involvement in class.

It's often the law

In 2000, the United States Congress passed the Children's Internet Protection Act, tying E-rate program discounts to a school's internet safety policy.

In England and Wales, the Department for Education issued statutory guidance "Keeping Children Safe in Education" in 2015, which requires schools in England to ensure appropriate filters and monitoring systems. A similar rule exists in Scotland.[4]

Similar measures are enforced in full or in part on every continent (excluding Antarctica, for obvious reasons).

System security

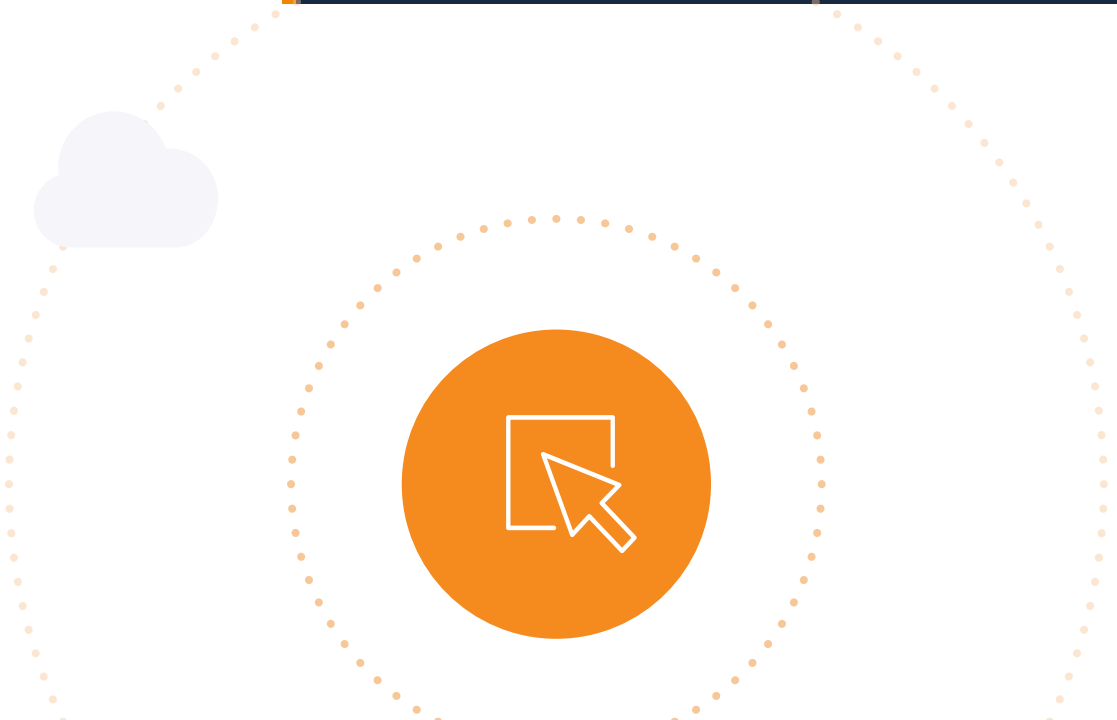
A filter that blocks malware, adware and spyware keeps students safe. It keeps your school's network secure, as well.

Monitoring and reporting

Parents need to have the reassurance that students aren't accessing content they want to keep them from, and schools must monitor their networks to keeping data and students protected.

But this has to be balanced with privacy protections and should be done without granular inspections of individual devices. This whole plan should be a transparent process of collecting anonymized data and presenting it to security professionals, parents and administrators.

Ensure that your school selects security tools that provide endpoint protection and network threat prevention such as Jamf Protect and Jamf Safe Internet. These should include protections for known viruses, behavioral analytics to find and isolate new dangers and thorough reporting. Ensure the tool you choose also has an involved community such as Jamf Nation or Jamf Educator where you can share best practices and get advice from others also striving for student success. Combine it with a comprehensive mobile device management (MDM) solution like Jamf School or Jamf Pro, and you'll be set.



Why not just block everything?

Statistics about vulnerable students could make parents and educators see locking down absolutely everything as an attractive prospect. But this can be a problem in a number of ways.

Teachers and students need access to sites that some schools may block in an overzealous attempt to protect students and preserve class time. YouTube or Google services, for instance, are part of many classrooms. Teachers who want to educate students on current events, social movements and many other topics find themselves frustrated when they are unable to access that educational content, and frustrated by a lack of ability to easily collect assignments digitally.

But unfettered access to these services can be a problem as well — you'll need a content filtering solution like Jamf Safe Internet that can filter in a more sophisticated fashion than simply by the domain name in order to both protect and educate students.

No filtering system is perfect. Someone has to find malware or phishing sites and add them to block lists, and unfortunately new sites are being created every day.

That's why preparing students for their futures on unrestricted devices should be a vital part of everyone's education. Young adults who already understand the potential dangers and know how to avoid harm will be safer online than those who were completely insulated from the internet by totally restricted access.

Students as Digital Citizens

A part of any student's education should include how to avoid phishing, malware, misleading information and more while on the internet — even after they leave schools and content filters.

Educating and training savvy digital citizens should be embedded within curricula and shape pedagogy. This includes how to understand what a reliable source is through a combination of critical thinking skills, education on what is and is not a trustworthy source—and the ability to avoid phishing and other scams.

If teachers are looking for a place to get started on helping students take ownership of their digital lives, we suggest the free ready-to-teach lessons, curriculum and ideas at Common Sense Education's Digital Citizenship program. Common Sense, a United States-based nonprofit organization dedicated to improving the lives of all kids and families, created these lessons in partnership with Project Zero at the Harvard Graduate School of Education. The lessons are divided into grades/age groups.

How to find the right filtering and security solution

How can you determine which solution is best for your school? Start with asking potential vendors the following six questions:

1 Does it filter all devices, including Chromebook, iPad and Mac? How about BYOD devices?

Solutions need to have full coverage in your school. A filtering system is only as good as its weakest wall.

2 How does it defend from unknown attackers?

Ensure that whatever system you use incorporates behavioral analytics and real-time alerts to catch unknown sites or malware, like Jamf Protect. Behavioral analytics can stop malicious actions by understanding how malware and dangerous sites take certain actions or use certain phrases.

3 Can it provide partial blocking on sites like YouTube or Google services?

YouTube and Google have become powerful learning tools, but can also offer a gateway to unfiltered content. You need a tool that ensures that Google Safe Search and YouTube Retricted mode are in place and can not be removed by the end user.

4 How does this solution keep parents involved?

While some parents might question the need for filtering at all, others may feel very anxious about any permeability whatsoever. Offering a parent the ability to see into the activity of their child's days through an app like Jamf Parent —as well as offering clear and detailed reports on security and privacy concerns such as those offered by Jamf — can help.

5 How does it filter student devices off-site?

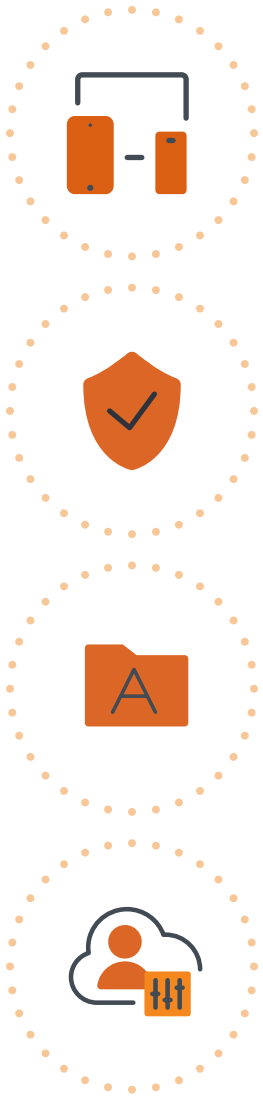
You want to ensure that whatever solution you choose, it incorporates filters and management for student devices at home, as well as school: just as Jamf School does. And it's even better if parents can increase the filters and management in an easy-to-use app like Jamf Parent.

6 How will it interface with my other solutions?

A filtering and security solution that can work seamlessly with an MDM provider and can partner with trusted vendors to offer not only world-class security but also increased educational options gives you a lot more for your money.

How can Jamf help?

Jamf provides solutions that both manage and secure your Apple technology. Beyond mobile device management, Jamf provides tools that support from an admin level through to parents, all while empowering students to succeed.



jamf SCHOOL

Empowering IT and educators with efficient Apple management

jamf PROTECT

Endpoint protection, purpose-built for Mac

Jamf Safe Internet

Purpose built content filtering and threat defense for education

Jamf Teacher

Jamf School Student

Jamf Parent

Jamf Assessment

jamf EDUCATOR

Customer education to support Jamf Teacher app

jamf MARKETPLACE

Valuable integrations that extend the Jamf platform

Jamf and Jamf Safe Internet can be an important tool in keeping students safe while maintaining privacy:

- **Jamf Safe Internet protects the end user, regardless of device as it supports both MacOS, iOS and ChromeOS**
- **Jamf Protect supports unknown attacks using analytics to monitor devices**
- **Jamf Safe Internet enforces the use of Google Safe search and YouTube restricted mode so users cant disable them**
- While Jamf Safe Internet is device-based and works beyond the school network, Jamf Parent also provides parents with additional tools to help secure devices away from school
- Respecting privacy: in addition to following all applicable rules and regulations regarding privacy, Jamf has signed the Student Privacy Pledge, highlighting our commitment to protecting the information of students, parents and teachers in our schools

jamf

The seamless, integrated experience of Jamf Safe Internet can add value to existing workflows in the Jamf Teacher, Jamf School Student and Jamf Parent apps.

Request a Trial

Or contact your preferred reseller of hardware.