familyzone.io

Most districts are dropping the ball with their web filter ...is yours?

Table of Contents

The Evolution of Web Filtering

We're coming up on 20 years since CIPA was enacted by congress and a lot has changed since then. There was a time when blocking pornography and a few other websites was enough for school districts, **but URL and reputation-based web filtering alone is simply not enough anymore.**

This eBook will dive into how web filtering has evolved these past 19 years and the steps your district should take to **stay up-to-date with the modern internet.**

The evolution of web filtering

Content filtering began in the late 90s, predominantly in libraries. Few people had the ability to access the internet in their homes, so it was common to rely on libraries to browse the web. With an unlimited amount of information at one's fingertips, the possibilities to grab content were endless. And this included pornography.

This posed unprecedented issues for libraries, where people feared children could potentially come across inappropriate content. Concerns and community pressure led to Congress passing the Children's Internet Protection Act (CIPA) in 2000 and President Clinton signing it into law in April 2001.

CHILDREN'S INTERNET PROTECTION ACT (CIPA)

CIPA requires any library or school receiving federal funding to adopt an Internet Safety Policy.

This includes a technology protection initiative that blocks children and adults from accessing visual depictions that are obscene such as pornography or anything that could be seen as harmful to minors.

supporting CIPA compliance

In order for school districts to receive E-rate funding, they must stay in compliance with CIPA. E-rate explicitly excludes refunds on content filtering, though, so it is a required technology cost. There are some attempts by the industry to include content filtering services within E-rate, but they have not been approved as of late.

The FCC requires three elements for compliance:

1. **Content filtering to prevent access to obscene, pornographic, or harmful images**
2. **Monitoring of online activities of minors**
3. **Education for inappropriate online behavior and cyberbullying awareness.**

Schools and libraries are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate content on the internet
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
- Unauthorized access, including “hacking” and other unlawful activities by minors online
- Unauthorized disclosure, use, and dissemination of personal information regarding minors
- Measures designed to restrict minors’ access to materials harmful to minors[1]

Thus, the business of content filtering for schools was born.

Content filtering is born

Shortly after CIPA was enacted, popular firewalls added web filtering to their lineup and new companies flooded the web filtering industry. Schools were primarily focused on pornography, with web filter companies focusing their pitch on the number of pornography sites in their database. Once pornography concerns seemed to be addressed, schools started focusing on gaming sites. This introduced the notion that the filter needed to be "smart" so that it could distinguish between appropriate, educational games and inappropriate, distracting games. Students got smarter as well. Around 2006, schools started identifying the use of circumvention to get around the filter as a concern.[2]

Types of filters:

- **Proxy Filters** - make requests on behalf of:
  - Explicit Proxy - typically defined in the browser
  - Transparent Proxy - proxy requests are made without browser interference
- **Transparent Filters** - allow clients to go to the web on their own, with the filter analyzing traffic as it flows. These typically scale better than proxy filters.
- **DNS Filters** - leverage manipulated DNS servers to deliver blocked pages for restricted content
- **Cloud Extension Filters** - use an extension for logged-in Google users but DNS for non-chrome OS or browsers

Each one of these filter types can be deployed in different modalities. The new wave of filtering combines multiple approaches to accomplish optimal performance and consistent policy distribution across multiple browsers and operating systems.

Circumvention

DNS filtering has come a long way, but can it still be bypassed?

The short answer is yes. **Students today are far more technologically advanced than they have ever been, and at younger ages.** This means that determined children know how to access VPNs, proxy websites and other anonymizer sites that are used to mask traffic and bypass the filter.

VPNs

Virtual private networks (VPNs) are a common way for students to attempt to circumvent the web filter that may be in place at school or at home.[3]

Example: *A student downloads a VPN onto a USB or on their phone when connecting to a school network. All the network can see is that this student is making an encrypted VPN connection and sending data via that connection. The specific VPN connection would have to be blocked in order to prevent the student from continuing that action. The problem is that schools enter into a game of "wack-a-mole" as a multittude of VPNs pop up every day.*

Top 10 VPNs Attempted to be Used by Family Zone Customers

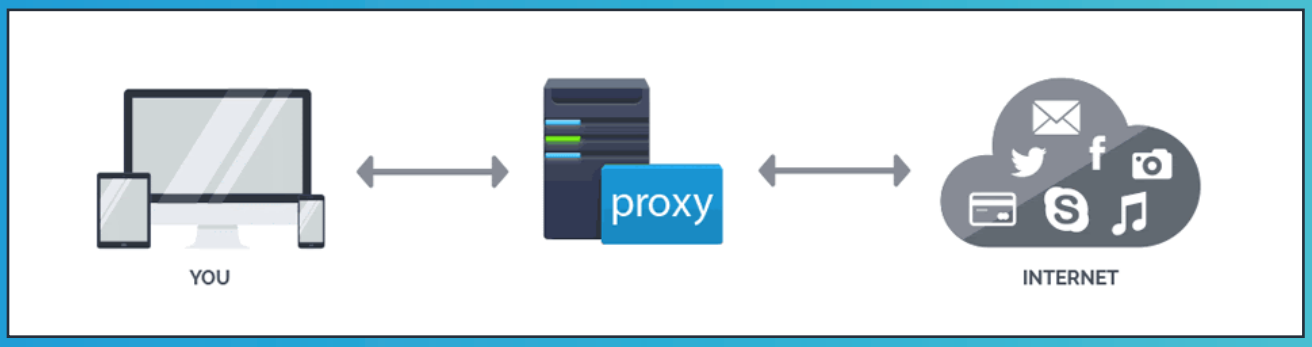
1. Ultrasurf
2. Psiphon
3. Tor
4. BetterNet
5. OperaVPN
6. Hotspot Shield
7. Tunnelbear VPN
8. Zenmate VPN
9. Chrome Browser VPN
10. DashVPN

Proxy Websites

In order to avoid installing anything on their devices, students are also looking to standard proxies to attempt to get around the filter. A proxy website is one that may look like **https://www.hidenseek.org/** for example, but when you browse there, it allows you to browse the internet freely without every changing the site in the URL bar. It is essentially a browser within a browser that doesn't reveal where the user is actually going. If they are looking to quickly access a blocked website, often times a proxy is the route to go.

Look Out For These Top Proxies Our Customers Are Blocking:

1. cIP-C
2. New IP Now
3. Hide.me
4. H1de
5. Proxy Site



Technology in the classroom

As students were growing up in a world flooded with technology, their schools started understanding the endless potential for introducing technological devices into the classroom to aid in the curriculum. Today, technology has become so prevalent in the classroom, that there is a paradigm shift in how students are absorbing content, knowledge, and being educated.

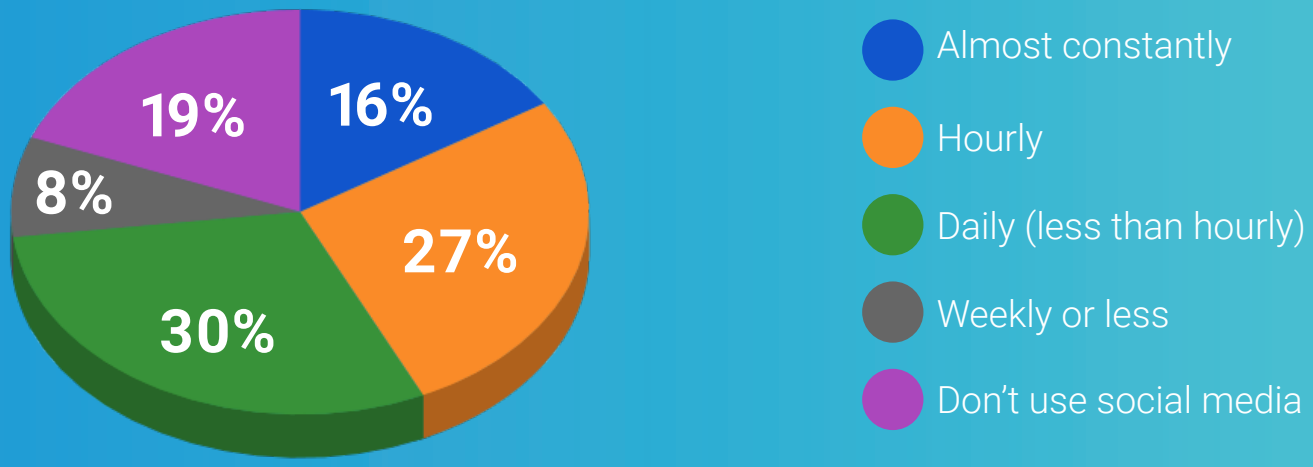
According to a study conducted by MidAmerica Nazarene University, only 42 percent of student work today is being done using a paper and pencil. Social media is now being leveraged as a form of education by many schools. Additionally, a report from Front Row Education shows great strides in schools adopting one-to-one programs.[4]

Social Media

It's no secret how prevalent social media is in our children and teens' lives, today.

Frequency of social media use, 2018

Among all 13 to 17 year olds, percent who check social media:[5]

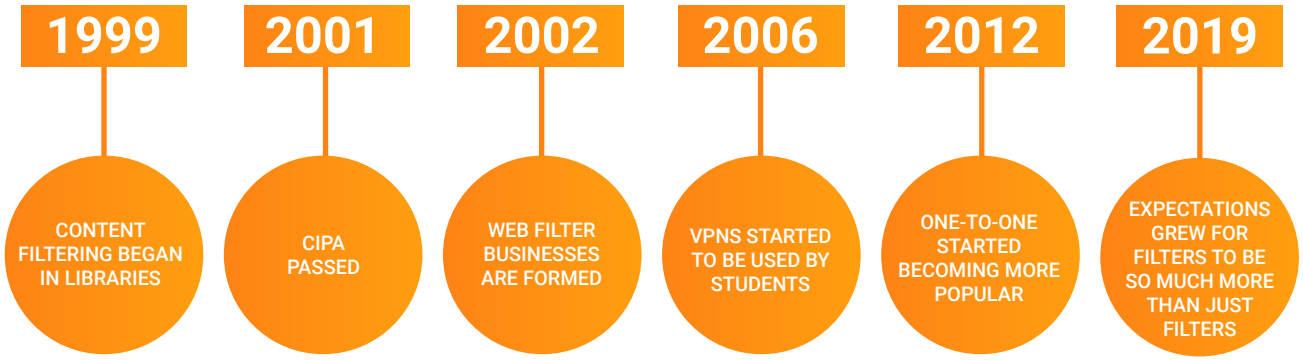


With students using social media so much in their personal lives, it only makes sense to leverage the platforms in teaching and learning as well. When used the proper way, social media in the classroom can aid in increasing student knowledge, improve communication among teachers, students and parents, and encourage student engagement.

One-to-one

A 2017 survey from the Consortium for School Networking reported 40 percent of districts in the U.S. were one-to-one. That's almost twice as many schools as in 2011.

This is promising for students, according to a Michigan State University study that shows providing notebook computers to students resulted in better outcomes in English, writing, math, and science.[6]



Concerns that increased technology brings

While leveraging social media for curriculum and implementing one-to-one programs are showing clear benefits to teachers and students alike, **great risks and concerns have arisen from those same initiatives.**

These include:

Cyberbullying

Distractions from the lesson plan

Students getting access to inappropriate content online

Students using the internet at school to search terms related to drug use, violence and self-harm

Increased load on strained technology departments

Technology admins making "curriculum decisions"

According to Act For Youth, **one in five** youth under 18 are exposed to unwanted sexual material online

Additionally, **over half** of adolescents and teens have been bullied online, and about the same number have engaged in cyberbullying.

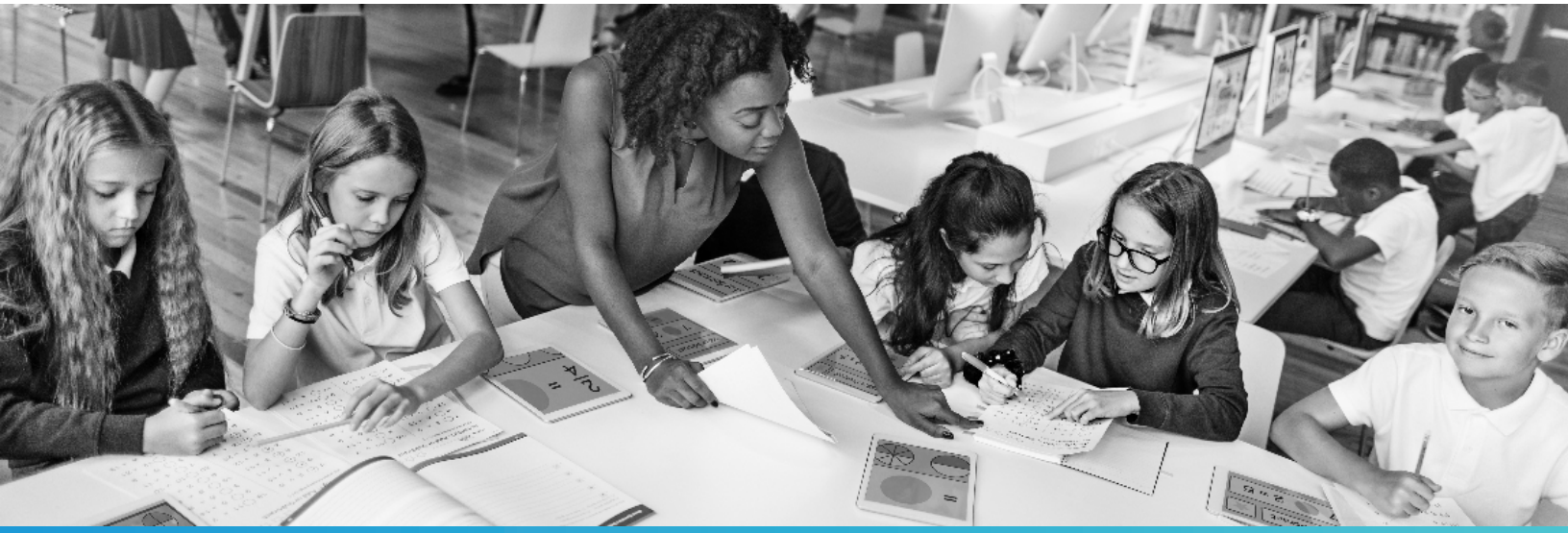
Unfortunately, **well over half** of young people do not tell their parents when cyberbullying occurs.

Going beyond CIPA compliance ...the complete solution

In the early 2000s, blocking pornography and some gaming sites was enough, but how has the changing landscape affected school needs?

Protecting students has become more complex.

We now have minors who have grown up only knowing life with the internet and social media. School districts must strike the right balance between safety and access to educational information.

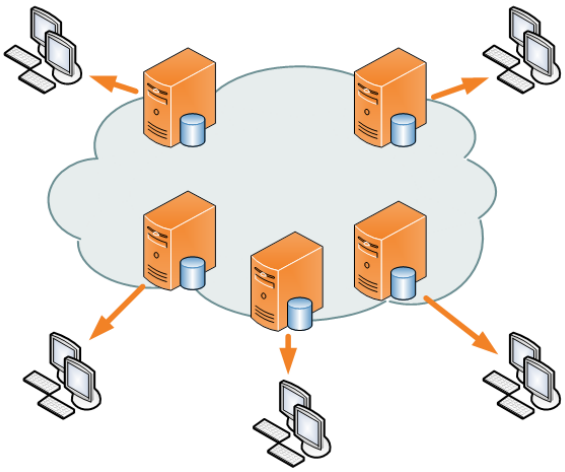


With the evolving complexity of the online landscape at schools, it's evident that districts **need to adopt more than just the standard web filter.** To thrive in the modern world, schools should be giving more control back to teachers, consider how they can leverage technology to support a cyber safety initiative for students, and leverage the data they're receiving from their web filter platform to educate parents and the community on how to keep children safe online.

The Internet isn't as simple as when your filter was designed

Five years ago, when you went to a company's website, you traversed their infrastructure, which meant using their web servers and assets within their data center. Using their own infrastructure was costly and time consuming; most companies had data centers with raised floors and rows of server racks, which constantly had to be refreshed and monitored. These costs were almost impossible for smaller companies to handle. Web filters were designed to give a reputation to every domain and URL. That worked really well before SSL, cloud hosting, and CDNs dominated the market.

Today, when you go to a company's website, you're really going to a hub of sites hosted all over the world in cloud infrastructure being delivered by many domains. This poses an issue for a reputation-based URL filter in all deployment methods. Why? Because those types of filters see all of the individual URLs and don't associate them with the main site being visited. In order to deliver dynamic content, many of those URLs are re-used by CDNs and web filters. If the reputation of one of the CDN URLs was associated with a blocked category in your filter, it would block the asset and break the website. This requires network admins to dig for blocked URLs in the logs and add them to their allow lists; probably one of the most time consuming tasks of a filter admin.



Filters for today and tomorrow need to recognize and associate all web/port assets with the services they are actually being used for.

This creates a smooth end user experience and removes tedious web filtering administrative load off of network admins.

Giving control back to teachers

It has become increasingly time-consuming and overwhelming for Network Admins and IT Directors to manage their web filter on top of the hundreds of other items they have on their plates. **The IT team shouldn't be acting as the internet police and certainly shouldn't be making curriculum decisions.** In a perfect world, IT would set CIPA compliance-related rules at a district level and then allow teachers and instructional technologists to control what type of content they want to allow at the classroom level. Tipping the balance of power back to teachers allows them to have more control over their curriculum and leverage the district's EdTech spend to its fullest, which ultimately benefits students.

According to the Software and Information Industry Association, K-12 districts in the U.S. spend about $8.4 billion on EdTech software per year.

Another adverse effect that many teachers are experiencing by giving each of their students devices in the classroom, is the difficulty of monitoring all the students at once. If there are 26 students — all using their own Chromebook — who are supposed to be reading an article online as part of the lesson, how does the teacher know they are not being distracted by virtually anything else on the web?

Classroom management software paired with the web filter gives teachers more visibility into what their students are actually participating in and gives teachers the ability to provide immediate feedback to their students.

Leveraging technology to build a cyber safety initiative

We now have technology that has the ability to block inappropriate content at a very specific level while also monitoring student behavior online, but how can districts leverage the data they are receiving from their platform to better protect their students? Monitoring search terms provides early indicating warnings that **students are contemplating self-harm, are bullying or being bullied, or participating in or planning violence at school.**

According to a CDC study, suicide is the second leading cause of death for ages 10-24, but **four out of five teens** who attempt suicide have given clear warning signs.

Over half of adolescents and teens have been bullied online, and about the same number have engaged in cyberbullying.

According to Counseling.org, one of the top early warning signs that school violence might occur is the **expression of violence in writings and drawings** by a student.

Alerting principals, counselors or school psychologists that a particular student might be showing early indicators or warning signs of being in a dangerous situation, can have a dramatic impact on keeping that student safe and potentially saving their life.

Educating the community on how to keep kids safe online

Web filters that go beyond CIPA compliance, provide teacher-level access for greater granularity and provide alerts to identify early indicators of trouble, are a great start, but a complete solution involves education. Technology can only go so far — **it takes a community to keep children safe** and that includes the education of teachers, students and parents alike.

Technology is fast-moving and often times parents don't know where to start when it comes to keeping their children safe and protected online. Today's parents typically look to their schools to provide that support and education.

Getting the most out of your EdTech spend

Billions of local, federal, and state tax dollars are being spent on district bandwidth, wireless infrastructure, switching, firewalls, chromebooks, licensing, web filtering, cybersecurity, and more. It's all to deliver a modern learning experience for our youth in order to prepare them for the world of tomorrow. However, many districts haven't thought about the reality of what that looks like in the classroom. Teachers are outnumbered by devices with distracted students and then content is blocked by a network admin that thinks they are just enforcing school policy.

One-to-one programs and a technologically advanced curriculum are great, but they're expensive. Districts are spending millions of dollars to ensure there is a device in each student's hands, and to make sure they can learn in a modern way, but seeing a positive return on these investments is key. Districts are dropping the ball if they're only blocking pornography. **With the influx of technology in the classroom, there do come risks in terms of safety and distraction.** Students have all the information in the world at their fingertips while in the classroom. This has forced web filters to be so much more than just web filters.

Here are a couple of examples:

Example 1:

An English teacher has developed a digital lesson plan that includes rich content with video, blogs, images, forums, and games. These elements are not violating CIPA compliance, but are still being blocked by the filter. The teacher then needs to reach out to their network admin, who is extremely busy, to unblock the content so they can deliver their lesson.

Example 2:

A language arts teacher has 30 children in their class who have all been issued Chromebooks. The teacher wants the students to read text online and then use a Google document to write a summary and their opinion about it. The student has access to their science homework they forgot to do last night and decides to do that instead of the lesson plan in their language arts class.

Summary:

The network admin's job is to keep the district compliant (CIPA COPPA FERPA) and to provide optimal performance of the internet.Teachers need complete autonomy over their classrooms to do what they do best...teach. Day-to-day curriculum should be handled by the curriculum department.

familyzone.io

Family Zone Platform

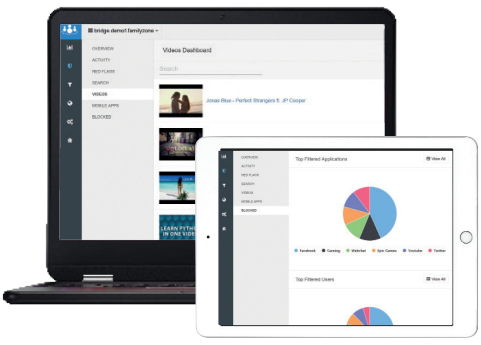
Familyzone.io is designed for today and tomorrow's internet.
We understand how the internet delivers content for today's educational environments and the foundation of our platform takes those needs into consideration to benefit all stakeholders; CTOs, Network Admins, Instructional Technologists, Teachers, Students, School Safety Officers, and Parents.

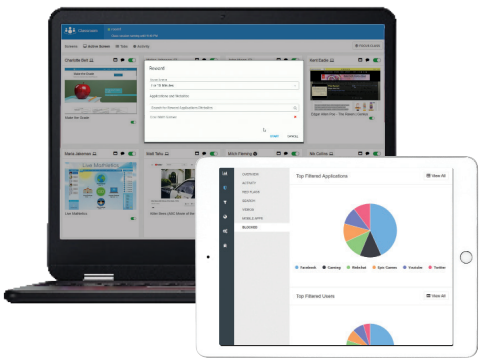
Familyzone.io provides a suite of three products to deliver modern CIPA compliance with student safety, classroom autonomy for teachers, and community engagement for parents to help keep kids cybersafe.

Family Zone School Manager

Family Zone Classroom

Family Zone Community





Family Zone School Manager

Cloud-managed content filtering that minimizes workload and maximizes compliance.

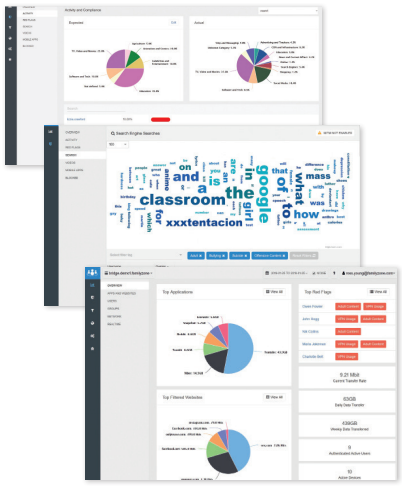
Supports all major operating systems on and off premise with feature parity, SSL visibility, scale, and consistency.

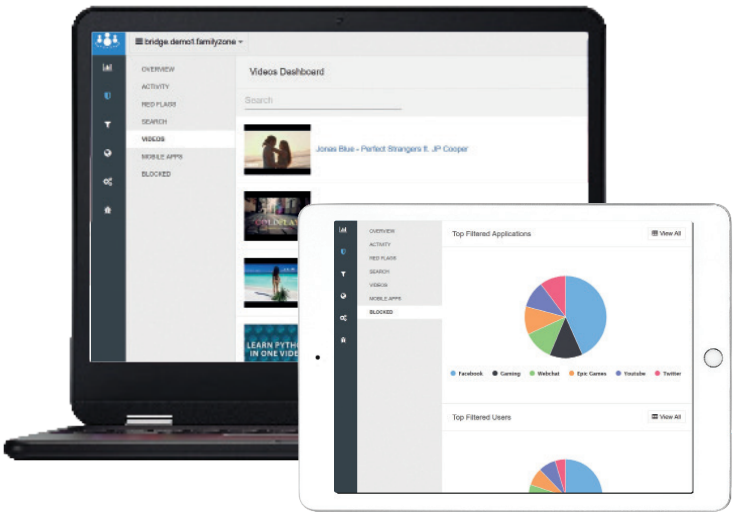
CTOs & CIOs:	Network Admins	Teachers And Students
• On/off-premise filter for scale that **supports all operating systems** and users • **Budget-conscious** consolidation of existing tools • **Free up your admin** from tedious filter tasks & empower non-technical admins • **Accepts identity from any providers** (SIS, Gsuite, Active Directory, Azure)	• Lock in **district-wide compliance** per group/ OU on either directory and on any operating system • **On/off-premise filtering** with consistency • **Gain deep technical visibility** on windows/ chrome/mac and access to macro reports • Limit time in the filter and **give control to teachers,** while staying CIPA compliant	• **Access to necessary resources** without being inhibited by filter blocks • **Smooth experiences** on educational applications leveraged for digital learning • **Easy-to-use** and navigate for non-technical users • **Get control** of your digital curriculum

Features

- Hybrid-cloud or full cloud deployment
- 10 GBPS support
- Native directory integration with G-suite, Azure, localized AD, LDAP
- Wifi authentication for G-Suite and AD users
- Filtering support for all endpoint operating systems
- Unique SSL visibility and controls without certificates
- Off-premise cloud filtering without backhaul

- QoS, bandwidth shaping, and quotas
- Cyber-safety reports with red flag alerts
- Packet-level visibility
- Radius integration
- AI and machine learning for VPN control
- Search term visibility
- Education-specific signatures
- QoS, bandwidth shaping, and quotas
- Cyber-safety reports with red flag alerts





"We were looking for a replacement for our existing content filter solution, and after much research settled on Family Zone. It is easy to administer with different levels of control being based on memberships in google groups and classrooms. Reporting is much easier to understand, as accumulated bandwidth is sorted by base url so educational resources like I-Ready that depend on various CDN's and 3rd party websites count referral links in as part of base URL. The dashboard is clean and easy to navigate. Overall, we are well pleased with our decision to go with Family Zone."

- Toby Bradley, Network Administrator, The Pascagoula-Gautier school district

Family Zone Classroom

Screen visibility + Classroom content control + Ease of use

CTOs & CIOs:	Network Admins	Instructional Tech. /Teachers
• **Relieve your network team** from making curriculum decisions in a compliant way. • Enable your curriculum department to leverage your technology investments to **deliver modern learning.** • **Budget-friendly tool** that integrates with your enterprise systems to ensure students are in the correct classes, independent of or in conjunction with Google.	• **Lock in your CIPA compliance** and let teachers deal with day-to-day overrides and lockdowns. • **Prevent teacher requests** and enable your teachers to get classroom control back through technology • **Integrate** with existing enterprise systems.	• Get classroom control back with **screen visibility,** content control and the ability to give immediate feedback to students • Ensure you are **getting the most** out of the digital curriculum resources. • Get **easy rollout** and training resources

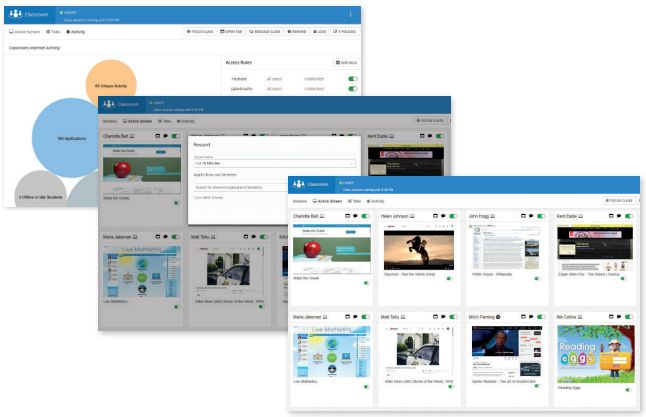
Features

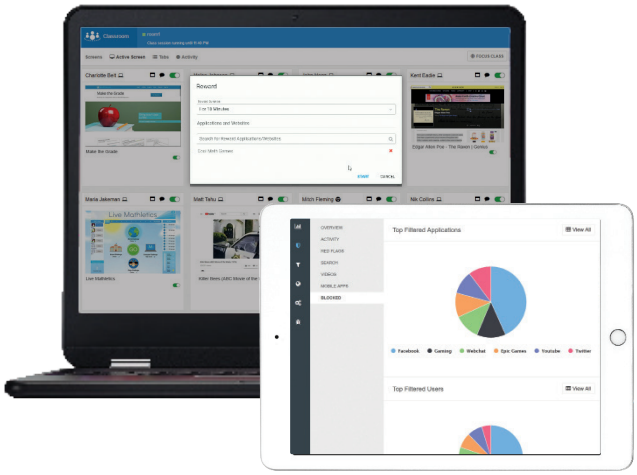
Allows Teachers To:

- See student screens
- See open tabs
- Message individual students or an entire classroom
- Open new tabs for class or students
- Focus the class, restricting access to specific sites or apps
- Turn the internet off for class
- Reward students by allowing limited-time access to sites normally blocked
- Create filtering policies for individual students or the whole classroom

Plus:

- Hybrid-cloud or full cloud deployment
- Google Classroom integration
- SIS CSV upload
- On-the-fly classroom creation with join code
- Teacher training hub
- CIPA-violation prevention with locked filter





"The Family Zone web filtering solution has been a great addition to our school district. Their modern approach to content filtering delivers increased insights into our student's web activity and provides an additional layer of security with its modern approach to content filtering for our 1:1 deployment. Most of all, our admins are spending less time administering this solution which allows more time to focus on other initiatives within the district."

- Demarius Gaither, Director of Technology, Fairfield County School District

Family Zone Community

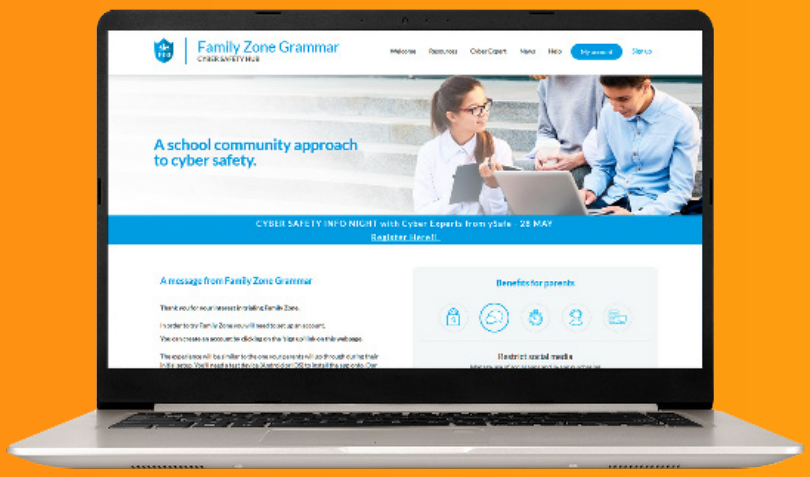
Digital parent education and training + Cyber danger warnings + School and community engagement

Familyzone.io is a global leader in both school and consumer filtering and we're excited to share our content with school and parent communities in the US.

Media Coordinator	Parent	Superintendent
• Empower your school district to be the thought **leader in cyber safety** education • One platform and content hub that **provides easy access** for simple content distribution	• **Free resource** for cyber safety education • Keep your children **safe online,** while getting insight into your children's online activity at school and at home	• Demonstrate to the community that you're **doing what you can for mental health,** school violence and keeping students cyber safe • Teach your student body how to be **digitally responsible** and gain political capital

Tactical Features

- ✅ **Online digital parent course**
- ✅ **Biweekly blog content**
- ✅ **Guided communication templates**
  - Social Media Posts
  - Emails
  - Flyers
- ✅ **Content hub (video, quizzes, visuals text)**



Conclusion

The evolution of web filtering is astounding when you think about where the industry stood fewer than 20 years ago. With change, though, there's often unease, roadblocks and concerns to overcome. A technology program that enables schools to keep their students safe online has gone way past a standard web filter.

That program must also include a mechanism to protect students based on their online behavior, a way for teachers to effectively monitor and control their classroom, and an educational initiative that **empowers the entire community to keep our children safe online.**

Connect with Familyzone.io to find out how ***one platform*** *can check all those boxes.*

https://www.familyzone.io/demo

familyzone.io

RESOURCES:

1 https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

2 https://infopeople.org/content/history-internet-filtering

3 https://www.howtogeek.com/167418/5-ways-to-bypass-internet-censorship-and-filtering/

4 https://blog.frontrowed.com/2016/11/17/2017-technology-in-the-classroom-survey-results/

5 https://www.commonsense.org/education/articles/what-new-research-on-teens-and-social-media-means-for-teachers

6 https://edtechmagazine.com/k12/article/2017/02/more-50-percent-teachers-report-11-computing