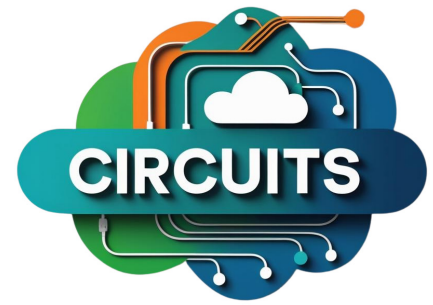




CLOSING THE DIGITAL SAFETY GAP: E-RATE AND THE EVOLUTION OF SCHOOL FILTERING

A MEMBER-ONLY BRIEF

Schools today operate in a digitally rich environment where safety, speed, and reliability are essential. School internet access is substantially more Protective/restrictive than what most students experience at home or on personal devices. Why? The reason is simple: schools that receive E-Rate funding are required by federal law to filter web content, and modern filtering systems make school-managed networks significantly safer than personal cellular or home internet connections. These protections are efficient, adaptive, and designed to keep students safe while still supporting learning.

Content Filtering Is E-Rated Mandated

Schools that receive federal E-Rate funding are legally required to implement web content filtering under the Children's Internet Protection Act (CIPA). Any school or district using E-Rate discounts for internet access or internal network services must certify each year that they have certified that they have an Internet safety policy that includes technology protection measures such as filtering. These technical protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors).

Content filtering is not optional. It is a condition of accepting E-Rate funds, and compliance is required for continued eligibility. However, decisions on filtering content will be dependent on the culture of the community and decisions of the school board. IT makes recommendations but the decisions on what to block is based on board and leadership. Districts may also decide to block materials based on grade and age level.

New CTOs need to understand community and administration values. What might be blocked in one community may not be blocked in another.

Why School Networks Are Safer Than Personal Devices

School network systems are significantly more filtered and safer than personal home networks, personal laptops, or student cell phones. School-issued devices benefit from district-managed protections that:

- Apply protections across all school-managed devices and accounts

- Apply regardless of where the device is physically located
- Block known categories of harmful content
- Enforce consistent safety policies
- Monitor emerging risks in real time

Are filters 100% guaranteed to stop students accessing inappropriate materials? No, there will always be a small subset of students who will use various techniques to attempt to bypass blocking. There is no technical product that will block a determined student 100% of the time. District CTOs are advised to go beyond filtering and monitor for obfuscation techniques, respond when students are identified using these techniques and work with school officials to address the student's actions as a behavioral concern.

Additionally, district leaders should be aware that protections provided on school devices do not extend to personal smartphones using cellular data. A student who brings a personal device and uses their carrier's network can bypass school filtering entirely. This is why students are safer accessing the internet on school-issued devices than on personal devices or cell phones.

How Modern Filtering Works

Today's filtering systems are faster, more adaptive, and more reliable than ever. They use:

- Machine learning and AI to identify concerning sites based on patterns, behaviors, and content signals, not just URLs
- Rapid response engines that can block newly discovered dangerous sites within seconds
- Ongoing updates that strengthen protection without slowing down the network

These systems can quickly put blocks in place when new threats emerge, and they automatically detect and restrict access to sites that fit harmful patterns even before they are formally categorized.

What Communities Should Need To Know

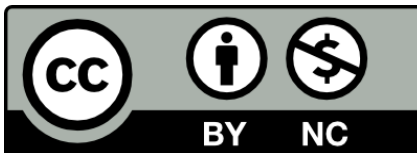
Schools that receive E-Rate funding are required to filter internet content, and this filtering makes school networks far safer and more controlled than anything available on personal devices. Modern filtering systems are increasingly sophisticated, using advanced machine learning to identify and block concerning content quickly and accurately.

Filtering is not the same as internet safety. While filtering can prevent access to web sites that meet the district's blocking criteria, filtering will not catch or prevent cyber bullying. Filtering is a safety net for students using the internet, not a first line of defense or a substitute for digital citizenship, setting clear expectations, and monitoring appropriate use. It is recommended that all school devices be configured to require content filtering, regardless of where the device is located. Because districts cannot require district filtering on bring-your-own devices (BYOD), personally owned devices should be blocked on the school network and the schools' Wifi network should be configured to also filter traffic and block content identified by district policy, limiting the possibility that students will access blocked content using personal devices on the school district's network.

As a result of carefully configured systems and protections, students using school-issued devices benefit from layers of protection that simply do not exist on personal cell phones using cellular data. When a small number of students persistently attempt to bypass these safeguards, the issue becomes more of an ethical concern rather than a technology failure, because the filtering systems are functioning as intended. These attempts can be tracked and monitored using the reporting and alerting capabilities available in web content blocking systems.

Knowing these requirements and capabilities helps families and administrators support safe, responsible, and compliant internet use in schools.

CoSN is vendor neutral and does not endorse products or services. Any mention of a specific solution is for contextual purposes.



Permission is granted under a Creative Commons Attribution + Non-commercial License to replicate, copy, distribute, and transmit this report for non-commercial purposes with attribution given to CoSN.

