ContentKeeper

White Paper

Ensuring Student Safety for Remote Learning

To keep students safe as they're learning remotely, districts need an Internet filtering solution that works just as well when students are learning from home as it does while they're at school. What's more, the solution should work equally well with all browsers and should enable visibility and reporting of students' online activity, regardless of what kind of device they're using.

As school systems make an unprecedented shift to online instruction in response to the COVID-19 pandemic, equity is a key concern. To ensure that students from economically disadvantaged families aren't left behind, districts are taking extraordinary steps to get technology into the hands of students at home.

For instance, South Carolina education officials are placing hundreds of school buses equipped with Wi-Fi in low-income neighborhoods around the state to serve as mobile hotspots for students. The Los Angeles Unified School District will provide Internet connectivity to as many as 100,000 students who don't have access at home. Many districts are supplying school-owned mobile devices for students to use so their learning continues uninterrupted.

While these measures are a good start, K-12 leaders also must consider how they'll keep students safe from accessing inappropriate content online. By law, any school receiving discounted Internet service through the federal E-rate program must use filtering technology to keep students safe when accessing the web through a school-issued device or network, and this applies whether students are on *or off* campus.

To keep students safe as they learn remotely, districts need an Internet filtering solution that works just as well when students are learning from home as it does while students are at school. What's more, the solution should work equally well with *all* devices and browsers and should enable visibility and reporting of students' online activity, regardless of what kind of device they're using.

ContentKeeper's Web Filtering and Security Platform for schools leads the industry in meeting these key criteria.

Remote Filtering Keeps Students Safe from Home

ContentKeeper allows administrators to enforce their school or district's Internet use policies remotely through a secure filtering profile on each device. This ensures that students have the ***same online experience from home*** as they have at school. What's more, administrators don't have to physically touch each device in order to provision it; instead, they can simply use Chrome, JAMF, FileWave, or any other leading mobile device management (MDM) solution to push out the profiles to student devices.

A Solution That Works with All Devices and Browsers

As Chromebooks have become the top-selling mobile devices in education, many school Internet filters have been designed specifically for the Chrome web browser. But a solution designed for Chrome isn't likely to have the same functionality with other browsers and device types — and that severely limits schools' options.

ContentKeeper has the same functionality whether students are using Chromebooks, iPads, Macbooks, Android tablets, or Windows-based devices, and it works the same with

Chrome, Safari, Edge, or Firefox. This means school systems can leverage *any* device type when distributing devices for students to use at home for remote learning and they'll still be fully protected.

Scalable SSL Decryption and Inspection

True cross-platform functionality requires a web filtering solution that can reliably decrypt and inspect Secure Sockets Layer (SSL) web traffic at very high speeds. This is something many web filtering solutions struggle with — but not ContentKeeper.

Because SSL decryption is so challenging, Google has developed workarounds that give schools some degree of control over Google and YouTube content through the Google "SafeSearch" feature. But this doesn't allow for detailed reporting of the specific web pages that students try to access, and it doesn't provide granular control over content within non-Google domains. In contrast, ContentKeeper can decode, inspect, filter, and log the full URL string for SSL-encrypted traffic at multi-gigabit speeds — providing the level of visibility and granular controls required for safe learning.

Granular, Policy-Based Control

Reliable SSL inspection enables the kind of granular control needed to safeguard students, eliminating overblocking or underblocking of websites. With ContentKeeper, this level of control extends to the content and specific subpages *within* a website, even if the site is encrypted. For instance, students are able to watch certain educational videos on YouTube — or read certain educationally appropriate material on social media sites — while still being restricted from the rest of those sites.

Meaningful Live and Historical Reporting

Managing digital learning effectively requires administrators to know what students are doing online and which sites and web applications they're trying to access in real time. ContentKeeper gives K-12 leaders comprehensive insight into students' Internet use, even when they're logging on from home on a school-issued device — with intelligent dashboards and advanced reporting capabilities that identify potential safety and network security threats.

Behavioral Analysis Adds More Security

Keeping students safe from inappropriate web content is important, but so is keeping them safe from physical harm. ContentKeeper's behavioral analysis technology monitors students' web searches for indicators of potentially harmful behavior (such as a search for "kill myself"), and if a match is found, an alert is sent to a designated administrator. These alerts capture the full *context* of the student's web search, which helps administrators quickly determine whether intervention is needed.

Contact Us

Please visit www.contentkeeper.com to learn more or schedule a demo.

ContentKeeper

ContentKeeper.com k12@ContentKeeper.com US: +1 888.808.6848
Intl: +61 2 6261 4950