



Best practices to shape & secure your 1:1 program

Contents

Dr. Jekyll	2
Mr. Hyde	3
Security & Productivity Best Practices	5
Best Practice #1: Secure Search	5
Best Practice #2: Secure YouTube	7
Best Practice #3: Secure Gmail & Chat	9
Best Practice #4: Delegate Web Filtering Policy to Teachers	10
Best Practice #5: Don't Just Block. Audit.	10
Best Practice #6: Delegate Web Filtering Administration to Principals and Guidance Counselors	11
Best Practice #7: Take-home needs Filtering or Parent Involvement	12
Best Practice #8: Layered Defense with Base Firewall Policy	13
Best Practice #9: Lock-Down Windows Devices with Active Directory	13
Best Practice #10: Lock-Down 1:1 Rollout with MDM	14
Conclusion	14
About Securly	14

Dr. Jekyll

Schools are adopting 1:1 programs by the masses. Every week, a number of districts make the news for deploying Chromebooks, iPads, and other devices.

Maine, one of the early adopters of a 1:1 initiative, distributed an Apple MacBook to every seventh- and eighth-grader in the state back in 2002. More than a decade later, its program has won qualified praise for making access to technology equitable across students of all socioeconomic backgrounds.

The 1:1 phenomenon is not just confined to U.S. borders – it is a global sensation. For example, the Malaysian government recently gave Chromebooks to over 10 million students across the country.

“As part of their 1:1 initiative, Malaysia is deploying Chromebooks to primary and secondary schools nationwide. These efforts to integrate the web are a central part of a national plan to reform its educational system.”

Felix Lin, Director of Product Management, Google



The benefits of a 1:1 program are plentiful:

- ▶ Devices have become cheaper than paper textbooks, and prices are continuing to fall. It makes financial sense for schools to re-allocate their resources towards buying devices; students will benefit from free 21st century online learning tools such as Khan Academy and CK-12.
- ▶ Online information is constantly evolving. By contrast, static textbooks become outdated.
- ▶ 1:1 programs allow students and teachers to remotely collaborate on projects via free online tools such as Google Docs.

Mr. Hyde

“Even the noblest of efforts — such as, say, the Los Angeles Unified School District’s program to give each of its 600,000-plus students Apple iPads — can suffer under the weight of bungled management. Since the district rolled out its \$1 billion program — funded by construction bond money ... reaction has ranged from skepticism at the beginning to down-right hostility as more problems were reported.” – Los Angeles Times

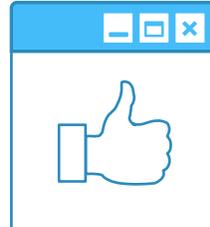
Several years and billions of dollars later, one question remains: are these devices actually being used for the reasons they were intended? Technology opens up a world of wondrous possibilities for students, but it also introduces new distractions and risks to a traditional classroom model. Among these perils is the growing threat posed by cyberbullying and online predators, along with unprecedented access to adult content through social media and other channels. This problem is further compounded when students take these devices home, where there is just a fraction of the supervision available at school.

Securly works with hundreds of schools across the United States to provide both in-school and take-home filtering. This enables us to see DNS, HTTP and HTTPS traffic from these schools “funneled” through a central location. Upending the traditional model (which asks for an on-premise appliance for reporting) allows us to have a centralized, high-performance repository for all of our customers’ audit data.

This helps us:

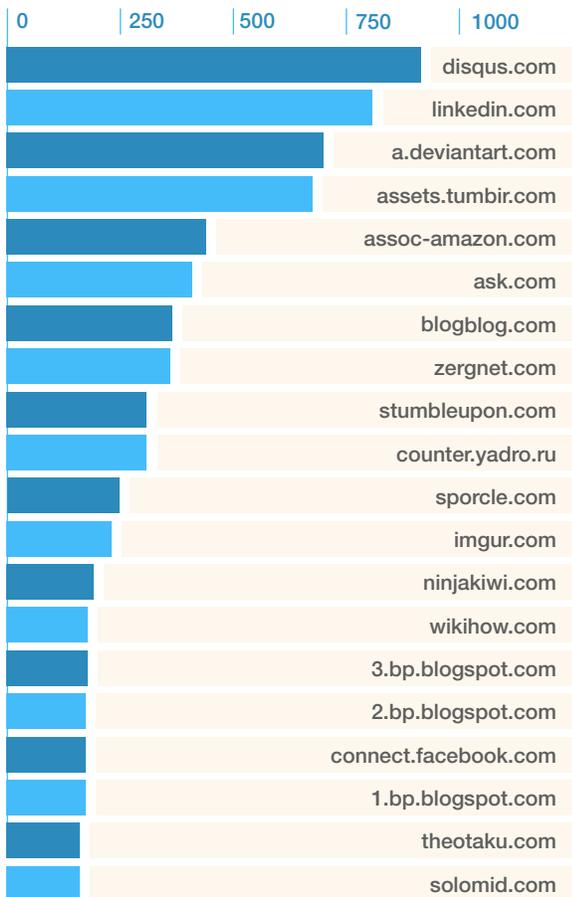


Find “needles” in any given “haystack” – Which students are being most productive or being blocked the most often?



Infer macro-trends among all of our “haystacks” put together – Which websites are most popular amongst high school take-home users across 100,000 students?

The following graph shows the in-school browsing pattern (top blocked sites) of one of our customer districts.



The browsing behavior of the same user cohort differs quite a bit in-home:



Facebook is by a long shot the most blocked domain at home. This shows that student behavior can vary considerably when they’re unsupervised.

Security & Productivity Best Practices

This section details several best practices we have learned from our customers in the field. We have seen these used time and again to create a safe learning environment while creating “buy-in” from all stake-holders (Administrators, Teachers and Parents) who are involved in signing off on a 1:1 rollout.

Best Practice #1: Secure Search

Turn on safe-search

Google, Bing and Yahoo support safe search on their respective search engines. A web filter will need to pro-actively enable these safety modes. We recommend enabling safety modes on these three search engines while keeping all other search engines (Ask, Duckduckgo, etc) blocked. The top three search engines already give students ample research opportunities for class assignments. Safety mode can be enabled by simply appending a string at the end of the URL, as shown here:



Google

?&safe=active

Bing

?&adlt=strict

YAHOO!

?&vm=r

Systems such as Dan’s Guardian and Safe Squid can be used to accomplish the above. For Chrome-books, turn on Google safety mode through the Apps for Education Admin Control panel. Additionally, Google has introduced a network based approach to turn on Safe Search called SafeSearch VIP.

SafeSearch Virtual IP address (VIP)

SafeSearch VIP will force all users on your network to use SafeSearch on Google Search while still allowing a secure connection via HTTPS. The VIP in SafeSearch VIP refers to a Virtual IP, which is an IP address that can be routed internally to multiple Google servers.



Note: the following has been excerpted from a longer version of Google’s KB article found [here](#).

When SafeSearch VIP is turned on, teachers and students at your school will see a notification the first time they go to Google. This lets them know that SafeSearch is on.

Note: Using SafeSearch VIP will not affect other Google services outside of Google Search.



Turn on SafeSearch VIP

To force SafeSearch for your network, you'll need to update your DNS configuration. Set the DNS entry for www.google.com (and any other Google ccTLD country subdomains your users may use) to be a CNAME for forcesafesearch.google.com.

Keyword blocking

Even with safe search turned on, keywords that would normally be inappropriate (ex: those related to drugs or violence) for a K-12 setting are allowed by Google, Bing and Yahoo. To address this issue, we recommend URL based keyword blocking. Securly uses a keyword list of over 1000 keywords that has been carefully culled to avoid False Positives. This list can be built from publicly available sources. We also recommend accounting for permutations of those keywords to address evasive behavior. For example, a student could type "h4(k1ng)" instead of "hacking" or "a\$\$" instead of "ass".

Safe Image Search

Several of our customers have reported the following issue: Image Search is not safe enough with Safe Search turned on. Blocking image search is not an option since there are legitimate uses for this functionality. In this case, turn on the "Creative Commons" filter. "Creative Commons" is supported by all major search engines and will filter out all images except those tagged as being distributed under the "Creative Commons" license. Based on extensive empirical evidence, we have found that images with this license are usually appropriate for classroom use. Further, the filter can be turned on for students only; staff image search remains unfiltered. The following strings will need to be appended to image search URLs to turn on the Creative Commons filter:

Google

&tbs=sur:fmc

Bing

&qft=+filterui:license-L2_L3

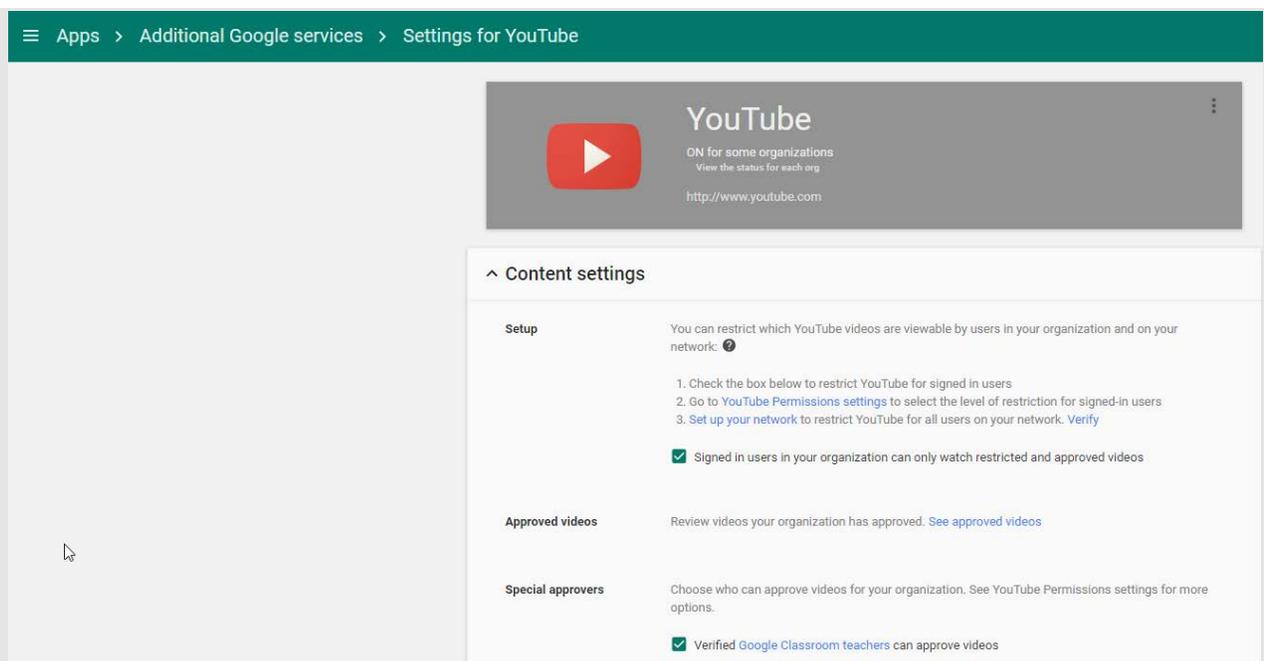
YAHOO!

&imgl=ccr

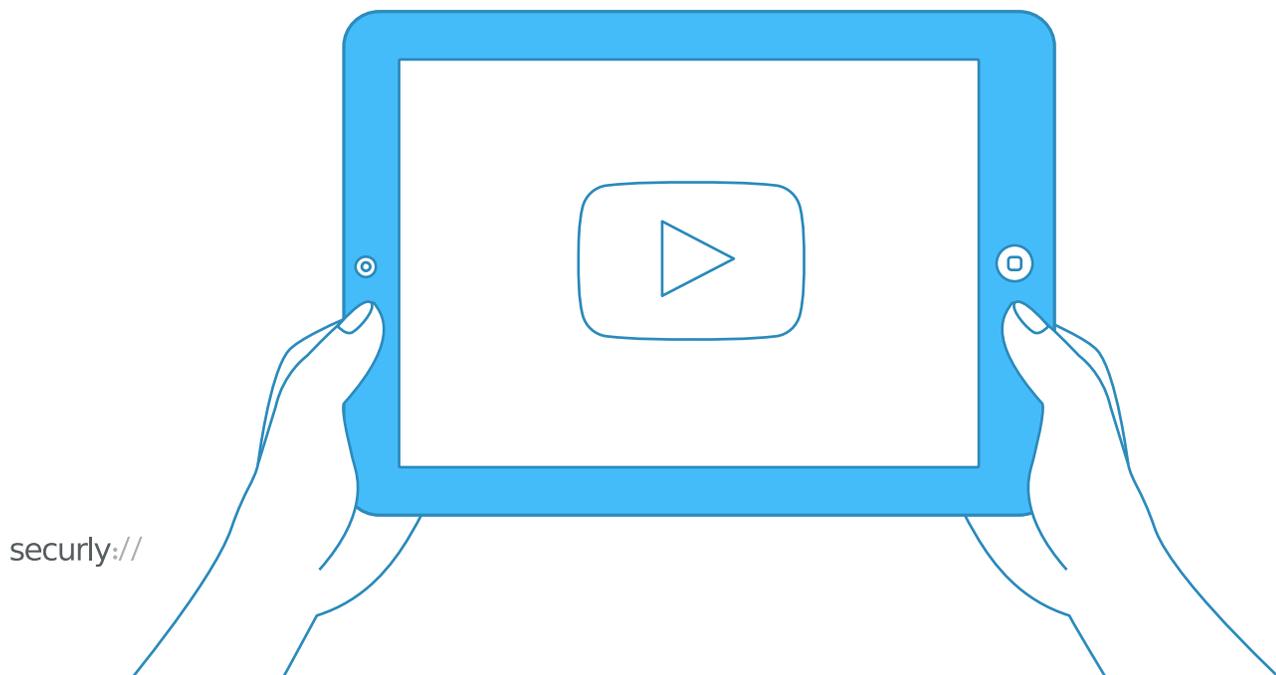
Best Practice #2: Secure YouTube

It is recommended to use GAFE to enforce YouTube Restricted so that Chromebooks will always get restricted mode. Using this method also allows your teachers to override blocked videos or entire channels. To achieve this: [Google Admin > Apps > Additional Google Services > YouTube](#).

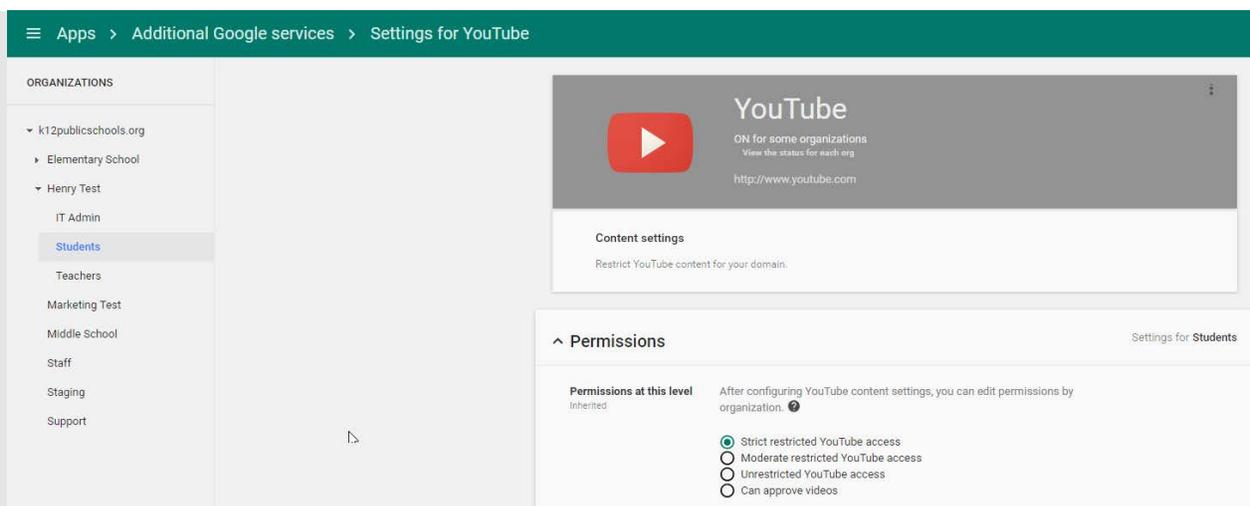
First select “Content Settings” and check the box for “Signed in users in your organization can only watch restricted and approved videos...” so that videos are restricted.



The screenshot shows the Google Admin console interface for YouTube settings. The breadcrumb trail at the top reads: Apps > Additional Google services > Settings for YouTube. The main header for YouTube is displayed, indicating it is 'ON for some organizations' with a link to 'View the status for each org' and the URL 'http://www.youtube.com'. Below this, the 'Content settings' section is expanded, showing three main areas: 'Setup', 'Approved videos', and 'Special approvers'. Under 'Setup', there is a checkbox for 'Signed in users in your organization can only watch restricted and approved videos' which is checked. Under 'Approved videos', there is a link to 'See approved videos'. Under 'Special approvers', there is a checkbox for 'Verified Google Classroom teachers can approve videos' which is also checked.



Then you may start configuring the settings for your OUs by selecting the permissions area:



Strict Restricted YouTube access



Enabled by default only when you choose the option “restrict content for logged-in users in your organization”.

Moderate Restricted YouTube access



Users can only watch restricted and approved videos. This offering is similar to the Restricted Mode setting in the YouTube app and offers a larger corpus of videos than the Strict offering.

Unrestricted YouTube access



Users can browse all of YouTube when signed-in even if you’ve also set network-level restrictions.

Can approve videos and channels



You can designate individuals or organizational units to approve videos and channels so that signed-in users in their organization can watch them.

For additional information on how your teachers can approve YouTube channels and videos, please refer to [this article from Google](#).

Best Practice #3: Secure Gmail & Chat

“Monitor the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications.”

– CIPA law (Source: fcc.gov)



The CIPA law is clear in its intent. E-mail sent by students needs to be policed. Since most web filters lack the ability to do this, schools normally end up blocking e-mail and chat. However, this is no longer an option with many schools turning to Google’s free Apps for Education (GAfE) suite as the foundation for their 1:1 initiatives. Part of GAfE is of course – Gmail – which students will need to use for a truly collaborative experience.

Auditor by securly://

To help IT Admins deal with the issues of cyberbullying and self-harm, Securly has introduced a FREE tool that uses Machine Learning techniques to monitor Google Mail and Chat for disturbing activity. At no cost to schools, Securly can also alert Principals, Guidance Counselors, and Parents of such activity.

Another challenge is that Gmail allows students to log in with their consumer (as opposed to Google Apps) accounts. Consumer accounts cannot be policed, subjecting the school to liability. The problem is complicated by the fact that all Gmail traffic is over SSL. Very few web filters support the ability to decrypt SSL traffic. Securly recommends the following steps to secure Gmail:



Intercept and decrypt Gmail related SSL traffic. Achieving this normally involves pushing out root certificates provided by your filter vendor out to your end hosts.



Add the HTTP header X-GoogApps-Allowed-Domains, whose value is a comma-separated list with allowed domain name(s). Include the domain you registered with Google Apps and any secondary domains you might have added.



Archive Gmail using an application like Vault. This makes all of the mail sent over your network searchable and keeps your school compliant.

Best Practice #4: Delegate Web Filtering Policy to Teachers

"Teachers need choice on when they're ready to unblock as they teach students to use technology appropriately." – Tanya Avrith, Google Certified Teacher.

We see two "classroom-level" issues come up time and again in post-deployment scenarios:

Classroom Management

This problem was solved with Windows-only applications like LanSchool. However, the product that we see used most often for a Chrome-heavy classroom is Hapara's Interact product.



Web filtering policy

The introduction of Common Core has allowed teachers much control over the tools and websites they use for classroom instruction. However, we believe that web filtering policy (which is decided at the district level) has not kept pace with this trend. More often than not, teachers find an interesting resource during lesson planning and discover the same resource is blocked during classroom instruction. The only recourse is to file a helpdesk ticket. We believe that where possible, teachers should be allowed –and encouraged– to tweak the district's web filtering policy to suit the needs of their classroom.

Best Practice #5: Don't Just Block. Audit.

"You can't change behavior that you can't see or connect to a specific user."
- Tim White, Director of Technology at Webb City R-VII School District

Based on our interaction with districts around the nation, we have come to the conclusion that filtering is not just about achieving compliance or denying access to students. It is about:



Modifying behavior. Being able to teach your students responsible use of the technology that they've been given access to.



Figuring out how students are **really using technology**. Usage patterns and statistics can be used to bolster community buy-in for scaling your 1:1 program.



Tweaking policies to reinforce positive behavior. If the initial policy is stringent, you might want to use evidence provided by your audit logs to open up access. On the other hand, if the policy turns out to be too lax and students end up spending more time than they should on distracting sites, you could use that evidence to keep them more focused on the task at hand.

Best Practice #6:

Delegate Web Filtering Administration to Principals and Guidance Counselors

While IT admins buy, install and maintain web filters on a day to day basis, we believe that in order for reporting data to be actionable, access to these reports needs to be delegated out to the right stake-holders. This includes Principals and Guidance Counselors.

Here's why:

In addition to routine requests for pulling user reports, district IT also occasionally has to respond to detection of disturbing behavior by students. For instance, a student's declaration to end her life through a Facebook post. Such incidents place immense burden on the district IT: they not only have to detect such incidents reliably, but also respond to them in a timely fashion.



By delegating this critical task of monitoring student behavior to the relevant staff members, the district IT is able to focus on infrastructure planning and remediating support tickets as before. Principals and Guidance Counselors can focus on their core responsibility of keeping students under their charge safe.

Best Practice #7: Take-home Needs Filtering or Parent Involvement

The need for web filtering is primarily driven by CIPA law. However, the law does not mandate filtering at home. Our customers who choose to filter at home do so because it aligns with the standards of their community. For school districts that choose not to filter at home, we do believe that a monitoring tool of some sort will be useful for the same reasons stated in the previous section. Without monitoring, you have no idea if your 1:1 program is 1) being put to good use or 2) on trajectory to do what it is really intended to do – raise student achievement.

In the absence of take-home filtering, several schools bring parents in as equal partners in 1:1 programs. Schools emphasize the shared responsibilities that parents have in ensuring that their kids are safe while at home. Organizations such as [Common Sense Media](#) offer out-of-the-box Digital Citizenship curriculum that you can use to engage parents around these issues. Securly offers a [Parent Portal](#) that allows your parents to monitor at-home activity on your devices as well as set policies.



Best Practice #8: Layered Defense with Base Firewall Policy

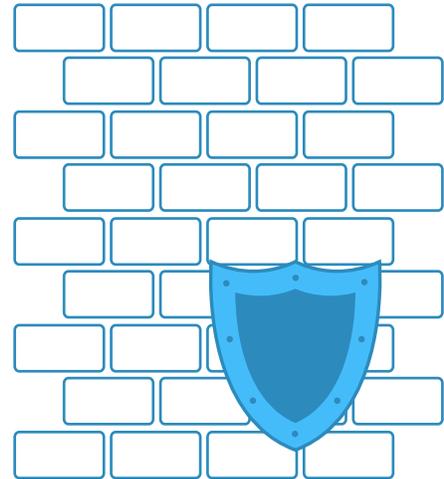
The following FireWall policies can be used with minimal effort to prevent the use of evasive applications and proxys in your environment:

Start out by keeping only ports 53 (UDP), 80 and 443 open on the egress and expand out from there. Generally speaking, DNS, HTTP and HTTPS are the only kinds of traffic you should see on the egress of your network. You could start from there and open up further ports based on user demand. Other protocols (RDP, FTP, etc) tend to be limited to your Intranet.

Blocking the HTTP CONNECT method will deter proxy access.

If you use DNS-based filtering such as Securly or OpenDNS, you can further lock down the DNS egress traffic to be limited to Securly/OpenDNS DNS IP addresses along with perhaps the clearing-house DNS server used by the district.

Likewise, if you are using a cloud-based proxy such as Securly or Zscaler, limit your HTTP CONNECTs to the IP addresses of Securly/Zscaler servers.



Best Practice #9: Lock-Down Windows Devices with Active Directory

In a Windows environment, you can prevent application installation by user group using GPO. Besides preventing the use of evasive applications, this has the added benefit of keeping malware off your network (and potential cost savings from not having to purchase anti-malware software for your Windows hosts).



Best Practice #10: Lock-Down 1:1 Rollout with MDM

We believe it to be self-evident that putting devices in the hands of your students without a way to manage those devices is unlikely to get favorable results for your 1:1 deployment.



Generally speaking, Chromebooks use the Google Apps Admin Control panel as their MDM. For Windows based devices, Active Directory makes it easy to push out Group Policies. The point of contention is mostly for iOS devices, per the lack of a good options from Apple. Common MDM options include AirWatch, Casper, JAMF and MobileIron. Several of our customers use Meraki's MDM simply because it is free and reliable.

Conclusion

While there is no silver bullet in security, the best practices outlined in this document will secure your 1:1 deployments against exposure to unsafe content. In addition, these tips will keep students focused on educational content and away from time sinks, thereby allowing your school to achieve a higher achievement ROI on your 1:1 investment.

About Securly

Securly is a cloud-based web filter that provides in-school and take-home filtering across all devices. For more information, please visit www.securly.com or email sales@securly.com

