securly://

best practices to shape & secure your 1:1 program

tech brief – summer2014 – v1.2

Contents

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. One of the better known deployments occurred in Los Angeles Unified School District (LAUSD), where 640,000 students would each receive their own school-issued iPad.

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. On the contrary, it is a global sensation. Take the country of Malaysia, for example, who recently gave Chromebooks for over 10 million students in 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 perceived benefits of a 1:1 program are plentiful, including:

- Given the constantly falling costs of devices, these have become cheaper than paper textbooks. This being the case, it makes financial sense for schools to re-allocate resources towards buying devices and have students benefit from free 21st century online learning tools such as Khan Academy and CK-12.
- Online information is constantly evolving as contrasted with static textbooks, where information is often outdated.
- Allowing students and teachers to remotely collaborate on projects via free online tools such as Google Docs.

Mr. Hyde

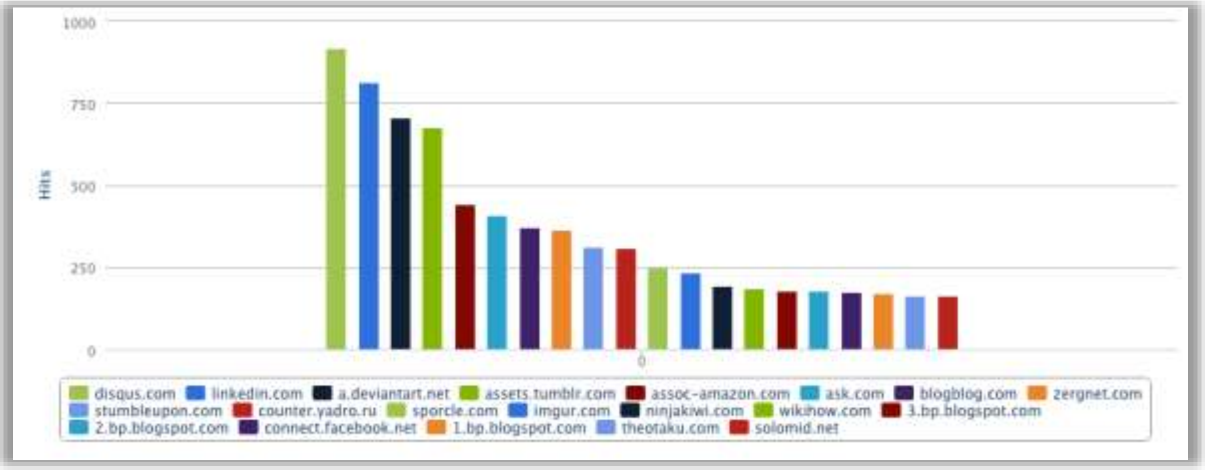
"Even the noblest of efforts — such as, say, the Los Angeles Unified School District's program to give each of its 600,000-plus students Apple iPads — can suffer under the weight of bungled management. Since the district rolled out its $1 billion program — funded by construction bond money … reaction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

– Los Angeles Times

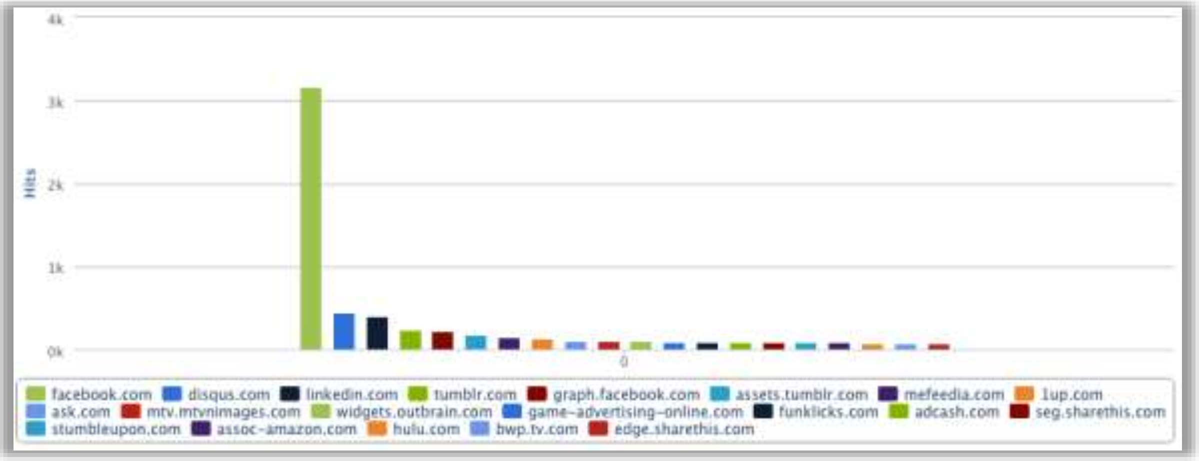
Several years and billions of dollars later, one question remains: are these devices actually being used for the reasons they were intended? There is no question that technology opens up a world of wondrous possibilities to students, but it also exposes them to distractions and risks that were previously less probable in a traditional classroom model. Among these perils is the growing threat posed by cyber-bullying and online predators, along with unprecedented access to adult content through social media and other channels. This problem is further compounded when students are taking 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 a on premise appliance for reporting) allows us to have a centralized, high-performance repository for all of our customers’ audit data. This in turn helps us find needles in any give haystack (Example: Which students are being most productive or being blocked the most often) or infer macro-trends among all of our haystacks put together (Example: 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 a district that is one of our customers.



The browsing behavior of the same cohort of users differs quite a bit as they go 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

We now proceed to talk about several best practices we have learnt from our customers in the field. We have seen these being 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 give students more than enough freedom to research on their 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. Chromebooks can have the safety mode turned on for Google on the Apps for Education Admin Control panel.

Redirecting encrypted search: In 2010, Google launched an encrypted version of its search engine that made SSL the default transport for all Google traffic. This was problematic for schools, as the Children's Internet Protection Act (CIPA) requires that students be blocked and audited when trying to access inappropriate content. Blocking encrypted search was not really a viable option, since Google has become a de-facto tool in the 21st century classroom. Google has instead provided schools with a nosslsearch.google.com option. All SSL traffic bound for google.com can be intercepted by the web-filter and re-directed to nosslsearch.google.com. This ensures a seamless re-direct from HTTPS to HTTP. Additionally, encrypted.google.com needs to be blocked by the web-filter because the nosslsearch trick does not work for this domain by design.

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 publically 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”.

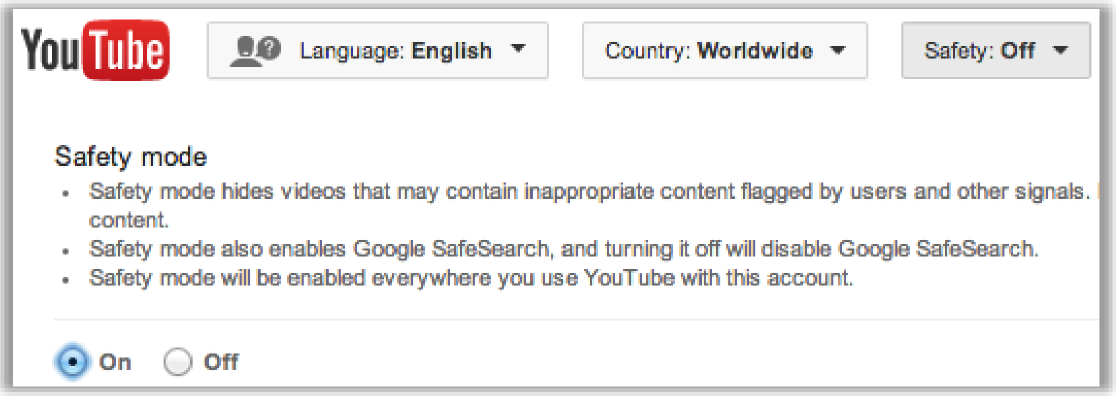
Safe Image Search: Several of our customers have reported the following issue: Image Search is not safe enough with Safe Search turned on. Blocking image search is not an option since there are legitimate uses for this functionality. Our recommendation in this case is to turn on the “Creative Commons” filter that is supported by all major search engines. The idea here is to filter out all images except those tagged as being distributed under the “Creative Commons” license. We have found based on extensive empirical evidence that images with this license are for the most part appropriate for classroom use. Further, the filter can be turned on for students only while leaving staff unfiltered on image search. 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

“So by enabling YouTube for Schools, you're limiting everyone's ability to see videos that aren't tagged as EDU or added to your own allow list. Then the list of people that are allowed to whitelist videos is something that you have to maintain manually” - I.T. Admin on Forum

There is often a debate in schools about the use of YouTube, with common implementations falling into one of three categories: completely open access, YouTube for EDU, or altogether blocked. Allowing students to access a completely open YouTube can expose them to potentially inappropriate or distracting content. On the other hand, YouTube for EDU tends to be limiting, as teachers and admins are required to add one video at a time to their playlist. With the undeniable importance of YouTube as an educational tool, blocking YouTube altogether is not really a feasible option. The solution we recommend: YouTube Safety Mode.



Language: English

Country: Worldwide

Safety: Off

Safety mode

- Safety mode hides videos that may contain inappropriate content flagged by users and other signals. content.
- Safety mode also enables Google SafeSearch, and turning it off will disable Google SafeSearch.
- Safety mode will be enabled everywhere you use YouTube with this account.

● On ○ Off

YouTube Safety Mode is a setting that, similar to Google's safe search, hides inappropriate content when enabled. Videos that have been flagged as being inappropriate by users for a host of reasons will not be accessible in this mode. The following string will need to be injected into the Cookie header of a YouTube traffic flow in order to enable Safety Mode:

- PREF=f2=8000000

What follows is a description of how two of our customers are using YouTube Safety Mode to achieve a conducive learning environment.

- Webb City R-VII School District, MO: Have turned on YouTube Safety mode for in-school filtering. Since the district believes that home is actually a *less* supervised environment, they turn on YouTube for Schools for their 1200 Chromebooks when they go home.
- Romeo Community Schools, MI: YouTube Safety mode has been turned on for both school and home for 3300 Chromebooks. The Safety Mode is used in conjunction with URL based keyword blocking to achieve a learning environment that is in line with community standards. Keywords that lead to inappropriate content showing up are blacklisted on an as needed basis.

Best Practice #3: Secure Gmail

"Monitor the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications." – Wording of the 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 on which they base their 1:1 initiatives. Part of GAfE is of course – GMail – which students will need to use for a truly collaborative experience. The challenge here is – allowing students to use GMail allows them to log in with their consumer (as opposed to Google

Apps) accounts. Consumer accounts cannot be policed and this opens the school up 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 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**: While this was a solved problem in a Windows-only world with applications like LanSchool, the product that we see used most often for a Chrome-heavy classroom is Hapara's Teacher Dashboard.
- **Web-filtering policy**: The advent of Common Core has meant that teachers have a great deal of control over the tools and websites that 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 who find an interesting resource during lesson planning end up finding that 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 indeed 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 for these districts, 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: Take-home needs Filtering or Digital Citizenship

The primary driver of the need for web-filtering is compliance with the CIPA law. Having said that, the law does not mandate filtering at home. Those of 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 to be useful for the same reasons stated in the previous section: without monitoring, you have no idea if your 1:1 program is being put to good use and on the trajectory to do what it is really intended to do – raise student achievement.

In the absence of web-filtering, we have found from empirical evidence that Digital Citizenship is an effective tool in encouraging appropriate use of technology resources. One example of digital citizenship as applied to 1:1 would be parents letting kids know that they cannot take devices with them to their bedrooms (an unsupervised environment). Many of the schools in our customer base do have programs in place that teach students appropriate use of technology resources.

Best Practice #7: Layered Defense with Base Firewall Policy

The following FireWall policies can be used with minimal effort to prevent the use of evasive applications and proxyies 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 clearinghouse 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 #8: 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 #9: 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 made it easy to push out Group Policies. The point of contention is mostly for iOS devices. The lack of a good option from Apple makes this the case. Common MDM options include AirWatch, Casper, JAMF and MobileIron. Several of our customers use Meraki's MDM simply because it is a free and reliable option.

Conclusion

While there is no silver bullet in security, the best practices outlined in this document can not only secure your 1:1 deployments against exposure to unsafe content, but also keep students productive and 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 support@securly.com