Content Filtering and the Unintended Consequences of Student Owned Devices

Eric Bylenga
IT Manager @ LCS
April 19, 2021

LCS has implemented a BYOD policy for our Gr. 7-12 students this year. Of course this means that every student will have at their fingertips a wealth of knowledge as well as a wealth of spiritually and personally destructive content.

So what do we do to protect our kids' hearts and minds? Often the first thought is to either deny access completely to everything or implement a content filter. In my experience as a parent and working in IT, there are problems with both of these approaches if used in exclusivity.

1. Complete denial of technology denies the reality that our children will at one point be exposed to the internet and technology that will most likely be used in their workplace and daily life in the future. While denial of access is a very simple solution, it could cause unhealthy use in the future when the child is finally exposed.
2. Content filters are good, but they're never perfect. No matter how good your filter is, your child is far more clever if they're determined to get around it. Whether that be through friends' devices or interesting hacks, there is simply no end to the ingenuity of our kids.

In reality we need to deal with not just a symptom of bad technology use but the root, which is in the heart (Jer. 17:9, Mk 7:21-23).

As Christians we recognize that we are sinful people and that even our children are tempted and often fail just as we do (Ge. 6:5,8:21, Ps. 51:5, Jn. 8:34). It is our responsibility to make sure that our children are reasonably safe from accessing content that will cause them to stumble and that there is a healthy dialogue at home regarding good digital citizenship (or GDC).

Here are a few thing that you can do to ensure the wellbeing of your child:

1. Put the devices to bed at night. When bedtime comes, devices also go to bed in an area off limits to your child.
2. Use the internet only in public places in the home. Create a public study place in your home where your child can work but will also be seen.
3. Restrict leisure hours on electronic devices. This will encourage other healthy habits not connected to technology.
4. Don't send your kids to a friend's house with their device and be aware of what devices friends are bringing when they're visiting.
5. Talk to your child about their use of technology, be aware of what services they are using and how they work.
6. Read privacy policies of the services your child is using or wishes to use.
7. Above all! Demonstrate good technology usage yourself! Practice what you preach!

A healthy use of technology should employ some level of technological safeguards. Here are a couple of devices and services that you can employ to protect you and your children from the unexpected.

1. Gryphon Connect: https://gryphonconnect.com/
    a. Powerful WiFi access point with great parental controls. Works with any device on your home network and is highly configurable for blocking and adding time restrictions.
2. Disney Circle https://meetcircle.com/
    a. Redirects all traffic on your home network through this physical device. Rules can be set up and traffic monitored on an admin console and again is highly configurable for blocking and adding time restrictions.
3. Qustodio: https://www.qustodio.com/en/
    a. App based content filtering and management. Good for Mac, PC, iOS, Android, Chromebook and Kindle.
    b. Uses a VPN to redirect traffic to a filtering server. Has been tested to work with the LCS network.
4. Covenant Eyes: https://www.covenanteyes.com
    a. Very similar to Qustodio with a focus on accountability. Good for Mac, PC, iOS and Android.
    b. Tested to work on LCS network.
5. AdBlockPlus: https://adblockplus.org/
    a. A great ad remover for those distracting and sometimes harmful ads on websites and Youtube as well. Not a comprehensive filter, but excellent for ads.
6. OpenDNS: https://www.opendns.com/home-internet-security/
    a. Simple to use but slightly more complicated to set up, but also fairly simple to circumvent. Good for a second layer of security but does not inspect search engine results.
7. CIRA Canadian Shield: https://www.cira.ca/cybersecurity-services/canadian-shield
    a. Similar to OpenDNS but Canadian. Only good as a secondary measure of security and should be set up on your home router.

And finally what is LCS doing to help your kids?

1. Starting in middle school, we've started the conversation on good digital citizenship. This has now continued into high school. In Grade 9, we talk about appropriate usage, privacy in regards to social media, search bias in services such as Google and the importance of living a life of integrity in the digital realm and physical world.
   This conversation will continue throughout the school year at all grade levels.
2. LCS implemented a Technology Use Policy in 2019-2020 which can be found in the parent handbook. Please give this document a read.
3. LCS employs two network content filters and firewall that uses blacklists, keyword triggers, heuristic analysis and decryption to block most of the bad stuff. It also employs a firewall that blocks most VPN services that kids use to circumvent the filters. As I'm sure you can appreciate while we do our best, no content filter is perfect, but we try!