

## **E-Rate**

All the dust has settled from our Category 1 filings. Category 1 covers our internet, WAN (wide area network connecting central admin, BHS, BMS and Babb and used to cover a portion of our telephone costs however telephone subsidies have now been phased out for all e-rate applicants regardless of our free and reduced lunch status.

For the 2019-20 fiscal year our Category 1 vendors will be:

- Northern Telephone Cooperative - internet Big Sky and Glendale Colony schools (remains the same).
- 3 Rivers Telephone Cooperative - internet - all campus locations except Big Sky and Glendale - migrating from 500 Mbps to 1 Gbps service (changing from Access Montana back to 3 Rivers, as previously stated the only reason we went to Access Montana 4 years ago for internet was speed. 3 Rivers at the time could only provide 100 Mbps service whereas Access Montana could provide up to 1Gbps service, today, 3 Rivers now offers 1Gbps service)
- Access Montana - WAN connections from admin to BHS, BMS and Babb. (this portion of Access Montana service remains the same)

## **Internet Filtering**

Who do we filter?

Prior to December 21, 2000 there was no requirement that schools and libraries provided content filtering on their networks. With the advent of e-rate at that time and courtesy of the late Honorable Senator John McCain who slipped a last minute amendment into the Children's Internet Protection Act (CIPA) of 2000, the requirement of content filtering in our schools and libraries became reality for those entities wishing to receive e-rate monies. The Children's Online Privacy Protection Act (COPPA) of 1998 is the other law often cited for content filtering but in fact contains the provisions for collection of personally identifiable information of children under the age of 13. COPPA is the reason companies such as Facebook require an individual to be 13 or older to establish an account.

CIPA law provides that schools and libraries filter for content in 3 broad categories in the law which are a) Obscenity as defined by *Miller v. California* (1973) b) child pornography as defined by 18 U.S.C. 2256 and c) content harmful to minors. The FCC provides broad guidance on these categories as many schools have interpreted this needing to filter services such as Youtube. The

## April 2019 Board Report

FCC has specific guidance on Youtube stating it is not required to be filtered because of CIPA but is rather a local decision. Yes in 2019, there are still many districts across the state and country that block or severely restrict access to Youtube and many other sites with valid educational content. The content harmful to minors category is open to broad interpretation by local school districts based on local community standards. Any other filtering/blocking decisions are made by local school districts for their own reasons such as blocking social media.

Interestingly enough, CIPA requires school districts to provide content filtering but offers no mechanism to pay for it and in fact specifically excludes content filtering from our applications for e-rate. As the e-rate program offers funding to both schools and libraries there are some entities that do not participate in e-rate so that they do not need to provide content filtering.

The BPS solution the past 4 years has been a Barracuda web filter appliance that all the districts internet traffic flows through and analyzed whether the various requests should be allowed or denied. Our web filter box also provides malware defense to prevent bad software from entering the district network by way of an internet download. As technology advances so it progresses in content filtering as well. While the Barracuda solution was the best choice at the time, as many resources have moved to cloud based solutions so have the best filtering solutions today moved to the cloud. Today's weaknesses of the Barracuda solution is that it is a physical device on our network subject to failure as is any piece of hardware and not being able to properly handle the onslaught of SSL (encrypted) traffic that now carries 85-90% of today's web traffic as well as the horrific reporting from Barracuda that is difficult at best to interpret. Why would BPS want to inspect SSL traffic through the content filter? The primary reason is to inspect traffic for malware issues that the Barracuda box is not capable of. The secondary reason is to analyze content for harmful issues and trends such as capturing the web activity of a student (or staff member) searching for self harm and/or suicide methods, what guns to use in school and other trends we unfortunately see in the nightly news. Sites such as social media sites, encrypted messaging apps are prime candidates for SSL inspection to detect descriptions of harmful activity.

On tonight's agenda (April 24) you will note one of the over \$10,000 purchases to iBoss. iBoss is one of the few vendors that tailors their service solely to the education market. The advantages that iBoss brings to the table for BPS is being a cloud based solution that iBoss can scale up or down to handle our internet traffic and SSL inspection needs so that we can be more preventative

## April 2019 Board Report

in malware attacks. iBoss also takes a full inspection approach to our internet traffic doing it's best to inspect for inappropriate content whereas other players in the market such as Securly and Lightspeed Systems only do URL inspections. CIPA also has the requirement that the district filter devices whether on the local network or taken home. iBoss provides the superior technology of certificate based filtering rather than the proxy based filtering we use today. And finally the reporting aspect, because iBoss is education focused, their reporting is education friendly as well as providing insight reports to safety issues to assist staying ahead and provide interventions to issues as may come to our attention.