NORTH PROVIDENCE SCHOOL DEPARTMENT **SCHOOL INTERNET CONTENT FILTERING POLICY**	First Read: 4/26/17 Second Read: Third Read:

SCHOOL INTERNET CONTENT FILTERING POLICY

4.1.1 Children's Internet Protection Act (CIPA)

In compliance with the Children's Internet Protection Act (CIPA), the North Providence School District has adopted and will enforce this Internet safety policy that ensures the use of technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) on all District computers, tablets, and smartphone devices with Internet access, as well as BYOD (Bring Your Own Device) computers, tablets, smartphones, or interactive projectors. Such technology protection measures apply to Internet access by both adults and minors with regard to visual depictions that are obscene, child pornography, or, with respect to the use of computers by minors, considered harmful to such students. The District will provide for the education of students regarding appropriate online behavior, including interacting with other individuals on social networking Web sites, chat rooms, and cyberbullying awareness.

4.1.2 WEB SITE FILTERING SERVICE

The School District will provide content filtering from a third party service, such as OSHEAN (IBOSS) or Cox Communications. This service is at a cost, and the filtering appliance is hosted in the Cloud and not on-site in the School District. Access to such appliance is given to the Communications and Technology staff via agreements with the third party vendor. At no time will any School District staff be given access to such system other than the Communications department to protect the security of students, staff, and administrators.

4.1.3 WHO IS FILTERED

The following devices are subject to filtering of internet content:

- Any District owned device connected to the Wi-Fi or Ethernet jack;
- Any Student (BYOD) device that is connected to the NPSD Guest Wi-Fi;
- Any Teacher BYOD device that is connected to the District Secured Wi-Fi or NPSD Guest Wi-Fi;
- All npsd.k12.ri.us email addresses.

4.1.4 FILTER CATEGORIES

The District internet is filtered into different categories based on the following groups:

- Administration
- Teachers
- Comms WIFI
- Students
- Guest WIFI

Each group is subject to different filtering rules based on work function.

4.1.5 NPSD INTERNET USE

- should support teaching & learning;
- avoid e-commerce, political lobbying, & hacking;
- should not disrupt computers or destroy data by spreading computer viruses or by any other means;
- obey laws and avoid plagiarism; respect copyright in all forms;
- be respectful & courteous; use appropriate language;
- does not compromise the personal privacy or safety of yourself or of others (especially students);
- does not post personal information/names with students' pictures;
- understands that emails and files are not private, and administrators and system operators may access any emails or files;
- violations will be reported and documented and by the Communications and Tech Department.

4.1.6 LOGGING INTO DEVICES

All district devices shall be logged in by the person who is physically using the device. **At no time shall teachers log into a computer with their personal accounts for the purpose of student use.** Every student has his or her own login and password. Individual logins record the person's activity and website access as well as content rules.

4.1.7 EMAIL FILTERING

Email filtering is provided by Google and through the admin console, PreK-8 students' email addresses are only allowed within the Districts npsd.k12.ri.us domain. Grade 9-12 students, teachers, staff and administers are allowed to email in and out of the domain. No teacher shall use a private or personal email address to conduct school business with other staff, students, parents, or any other vendor or agency. Teachers will always use their npsd.k12.ri.us account.

4.1.8 SITES THAT ARE BLOCKED

- Sites offering pornographic, sexual, or adult-only content and any that are inappropriate for minors and violate CIPA;
- Sites allowing unmoderated uploading of images, photos, & videos inappropriate for minors;
- Sites promoting cheating, illegal drugs & paraphernalia, and any other illegal activities;
- Sites that engage in phishing, pharming, fraudulent, & malicious content;
- Sites that are proxy, circumventor, & bypass that allow viewing of blocked sites;
- Web page translation and caching sites that allow viewing of blocked sites;
- Sites promoting hate, discrimination, violence, terrorism, bomb-making, and/or inappropriate use of weapons;
- The Social networking site called *Snapchat.*

4.1.9 BLOCKING/UNBLOCKING WEBSITES

Due to the very dynamic nature of websites, content filtering solutions are never 100% accurate. An unlimited number of site and page content changes are posted to the internet daily, sometimes resulting in a delay before inappropriate sites are identified and added to the databases. Conversely, an appropriate site may be blocked for various reasons. In particular, when a normally appropriate site is hosted on a server that also hosts inappropriate sites, all sites on that server may be blocked

At the discretion of the Superintendent, the Assistant Superintendent, the Curriculum & Technology Integration Specialist and/or the Communications Director, any web site can be blocked to students or all teachers and staff, based on its content or questionable security that may possibly disrupt the district computers or network.

Any Teacher who needs a web site unblocked must put the request to the Curriculum & Technology Integration Specialist or Principal, who will put in a work order to the Tech Dept., requesting the said site be examined by the Curriculum & Technology Integration Specialist and Communications Director to be unblocked. If at any time the site is questionable to violate said policy, the Superintendent will make the determination of approval or denial.

4.1.10 NOTIFICATION OF INAPPROPRIATE ACTIVITY

The content filter system creates logs that are generated and accessible by the Communications and Technology Department that will allow them to search each user as to what website they have visited or requested and it will also alert the Communications and Technology Department of certain sites and search requests that are deemed threatening and of urgent concern to the safety of the students and staff. At any time, an alert is received the Superintendent and Assistant Superintendent will be notified. If they cannot be reached, then the school principal will be notified, and the Communications and Technology Department will then copy any log files and emails from involved persons, if known, and await further instructions.

Even though the content filtering system blocks most inappropriate sites, it does not protect the students for all inappropriate content or pictometry. Teachers shall always monitor and do due diligence to what a student is viewing and surfing on their computers and report such inappropriate activity to Principals.

A student found to be intentionally conducting inappropriate activity or viewing inappropriate sites on a device shall be subject to discipline, as described in the student handbook.

4.1.11 LOGS AND NOTIFICATIONS

The system provides history logs of all users connected to the internet on locations visited, and all emails sent and received, and their accompanying content. At no time shall any email information be requested by anyone, except for the Superintendent or Assistant Superintendent to the Communications Director. At no time is a Teacher, Principal, or staff member allowed to request such information to the Communications Department staff other than the Director.
Such logs shall be searched by the director on a quarterly basis to review for inappropriate or illegal activity. Any such activity found shall be reported to the Superintendent. At any time, if the Police Department requests information from logs for possible criminal activity, the Superintendent or Assistant Superintendent shall first authorize approval, unless notification time would impede the police in an investigation that pertains to the safety of students, teachers, or staff. At that time, the Communications Director shall relinquish any and all log info that is requested by the Police and continue to try to contact the Superintendent.