NORTH PROVIDENCE SCHOOL DEPARTMENT SCHOOL INTERNET CONTENT FILTERING POLICY	Approved: 7/26/2017

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.

WEB SITE FILTERING SERVICE

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

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 or chromebook wi-fi;
    - Any teacher BYOD device that is connected to the District Secured Wi- Fi or NPSD Guest Wi-Fi;
- All NPSD email addresses and google accounts

FILTER CATEGORIES

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

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

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

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 any individual (especially students);
- does not post personal information/names with students' pictures;
- understands that emails and files are not private, and that administrators and system operators may access any emails or files;
- violations will be reported to and documented by the Communications and Tech Department.

LOGGING INTO DEVICES

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 a personal login and password. Individual logins record the person's activity and website access as well as content rules.

EMAIL FILTERING

Email filtering is provided by Google and through the admin console, PreK-8 students' email addresses are only allowed within the District's email domain. Grade 9-12 students, teachers, staff and administrators are allowed to email to and from 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 District email account for school business.

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

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 or the Communications Director, any website 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 website unblocked must submit the request to the Principal, who will submit a work order to the Tech Dept., requesting the said site be examined by the Communications Director to be unblocked. If at any time the site is questionable and may violate said policy, the Superintendent/designee will make the determination of approval or denial.

NOTIFICATION OF INAPPROPRIATE ACTIVITY

The content filter system creates logs that are generated and accessible by the Communications and Technology Department that will allow staff members to search each user as to what website they have visited or requested and it will also alert the Communications and Technology Department when inappropriate or blocked activity is attempted by the student, teacher, or staff member. A review of these logs will occur and the principal will be notified if deemed necessary regarding the student activities; and the Superintendent office shall be notified if deemed necessary for any teacher or staff activity.

The content filter system also creates log and notifications when it detects specific inappropriate keywords that are deemed threatening or urgent concern to the safety of the students and staff. These email notifications are received by the school principals who also may require the notifications to be sent to certain staff members such as school social workers or psychologists. It shall be noted to all parents/guardians that these alerts are sent to principals and or staff via email and it shall not be presumed that these emails are monitored continually each day. It shall also be noted that these email alerts are NOT monitored after school hours including nights, weekends, holidays, and during vacation breaks. Once a principal or staff member reads an alert message, the principal shall take appropriate action to investigate the alert and determine if any action or interaction shall take place.

Even though the content filtering system blocks most inappropriate sites, it does not protect the students for all inappropriate content or pictometry. Teachers should frequently monitor what students view and search on their computers and report any inappropriate activity to the principal.

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

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. Such logs shall be searched by the Director of technology 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.

Approved: 7/26/2017

Revised: 6/23/2021