



Safe Technology And Digital Citizenship

**updated 10-16-19*

- **What filters are being used and how do they work?**

Washington County School District Technology uses iBoss content filters for all inbound and outbound traffic. iBoss is supported and funded in part by the Utah Education Network (UEN). UEN pays for the subscription service to keep filters up to date regarding new and changed content on the internet. District Technology pays for the appliances that provide the filtering. All internet traffic coming into and out of the district is channeled through the filters. The filters consist of both software and hardware components. There are several algorithms used to filter content. At the top level a subscription to a list of inappropriate sites is maintained and all content coming from those sites is blocked and the user is notified of the filter blocking. At the second level sites that are allowed through are checked for key terms that are either inappropriate or suggest inappropriate content such as bomb making or other illegal activities. The District has purchased a pair of filters to allow for both redundancy and increased capacity.

- **Are there different settings used for different grades and school levels?**

At this point in time, filtering is not based on grade or school levels. All content is filtered the same way for students, as well as teachers and administration.

- **What is the district filtering policy on frequently used sites such as YouTube, Google Images, Weebly, and etc.?**

Besides the iBoss filters, District Technology also manages Google filtering on both YouTube and Google Images. Google filters for both have gone through some significant changes in the last year and have become much more restrictive. We are able to allow teachers to manage content permissions on YouTube. Other content for popular sites is filtered through standard iBoss filtering protocols.

- **Are there management systems available (MDM, Chrome management, LanSchool, and etc.) that can add additional control and who accesses those systems?**

Schools are requested to purchase management with all Chromebooks. Chromebook management is a tiered management system with the highest level managing all Chromebooks, and then school and teacher levels of management to manage what applications are available and user access. The District owns a LanSchool license that can be used on almost any device and is available to all schools. iOS management is slowly evolving. We are hoping that by the end of the school year we have a full district level management system in place for iOS devices. At this point in time, iOS management is taken care of at the school level.

- **What resources does the district provide concerning educating students on safe internet use and digital citizenship?**

At the elementary school level, all lab aides are provided with and taught how to use and teach online internet safety, security and privacy. District Technology provides the elementary lab aides with numerous resources for this purpose. The lab aides also meet once a month to discuss changes and any new issues dealing with internet safety and security.

District Technology has not been able to successfully develop a program for secondary schools because each school and set of grade levels do not permit us to set training up in any kind of consistent format. It is District Technology's recommendation that each school go through the content at [commonsensemedia.org](https://www.commonsensemedia.org) and establish a digital safety, citizenship, privacy and security program. There is a professional development piece for teachers, as well as instruction for students.

<https://www.commonsensemedia.org/educators/scope-and-sequence>

District Technology has developed and provided a set of guidelines/policy for schools that choose to support BYOD (Bring Your Own Device). The guidelines provide an adequate amount of information with regards to how BYOD should be implemented. It is strongly recommended that secondary schools implement the BYOD guidelines because students are going to be bringing devices to school even if the policy is not implemented.

- **What is the protocol in district schools when inappropriate content is accessed for students, employees and parents?**

Policy governing student, and staff use of District technology resources is covered in [District Policy 3700](#). Consequences for inappropriate use are covered in this policy. Misuse of resources that violate either state or federal laws must be reported to the appropriate district administration. In the case of employees, law violations must be reported to Human Resources. Otherwise, it is up to the school administration to determine what discipline measures should be taken.

- **Explanation of district capabilities or inability to change filtering, settings and management tools based on best practices, technological limitations, and funding. Where applicable, districts could include what is provided in connection with e-rate funding.**

HB 213 was put into law without any additional funding to support the mandates of the law. A more sophisticated level of filtering could take place; however, a reallocation or additional manpower would be necessary to accomplish this task. E-rate funding requires that all internet access is monitored, and it is assumed that filtering meets the requirement of the regulation. It is important to recognize that filtering is only part of the monitoring solution. District Policy 3700 states that devices connected to the internet that are being used by students on school property must be physically monitored by the teacher/adult responsible for the students when they are using the devices. Other programs can be purchased such as NearPod that allow teachers to put students into a managed environment, but nothing besides LanSchool has been purchased at the district level for this purpose.

- **What devices are being used and how are classes using them?**

***SmartBoard or Promethean Board** in each classroom (Preschool through 5th Grades)

*All teachers use their board on a consistent/daily basis for curriculum and student interaction

***Elmo display projector** in each classroom (Preschool through 5th Grades)

*Primarily used in lower grades, but all teachers have one in the classroom; teachers are able to project what they are doing up on the SmartBoard/whiteboard so ALL students can see

***Chromebooks**

*iReady software (3rd, 4th, and 5th grades)

*Lexia software (Kindergarten, 1st grade, 2nd grade)

*Waterford software (Preschool)

In addition to the above mentioned devices, each grade-level also has:

Preschool: iPads used for educational games such as Starfall and Osmos used during independent centers and the work table at the end of the year

Kindergarten: 25 iPads per classroom (language arts, math educational games; iPads are not updated high enough for Lexia this year); Osmos for daily center time; 6 chromebooks per class used for Lexia

1st Grade: two classroom sets of chromebooks (30 per set) used for software such as Lexia, Imagine Learning, and Kahoot; 6-8 iPads per classroom used for QR Code reading during center time.

2nd Grade: two classroom sets of chromebooks (30 per set) used for software such as Lexia, Imagine Learning, Spelling City, and writing apps; 2 laptops per classroom for extended learning opportunities and Imagine Learning (ELL students); Chromebook portable labs used for research, Microsoft Word, and PowerPoint for students

3rd Grade: 1:1 chromebooks for SAGE/RISE Modules and testing, Reach for Reading (R4R) & MyMath software, iReady, Spelling City, writing and keyboarding work.

4th Grade: 1:1 chromebooks for Spelling City, iReady, center work, writing, STEM, interventions, research, and reading

5th Grade: 1:1 chromebooks for Daily 5 center time, SAGE/RISE Modules and testing, Reach for Reading (R4R) & MyMath software, iReady, writing and keyboarding work.

• What are the main applications, programs, and sites used in different classes, grade levels, and subject areas?

Preschool: All students work in language arts in a software program called Waterford.

Kindergarten, 1st Grade, and 2nd Grade: All students work in language arts in a software program called Lexia. iPads have different educational games that have been approved for language arts and math subjects.

3rd Grade, 4th Grade, 5th Grade: All students work on language arts and math in a software program called iReady. iReady is also offered before and after school to students if parents are able to bring them before school or pick them up after school.

Preschool: ABC, math & sight word games, ABC Ninja, Little Writer, Letter School, Number Magic, Preschool Math, Vehicle Number Trace, Spelling 1-4, Sight Words by Little Speller

Kindergarten: iPads have various apps approved by teachers for math and Language Arts; students are locked into an app when using the iPads; Class Dojo; Brain Pop, Jr.

1st Grade: Class Dojo, Lexia, code.org, Epic! and other reading and math apps, Brain Pop, Jr. Story Bots, QR Codes.

2nd Grade: Class Dojo; Kahoot!, math/language arts apps, research and PowerPoint on chromebooks; Brain Pop, Jr., Lexia

3rd Grade: Class Dojo, Review apps for language arts and math, Kahoot!, Google Docs, Google Slides, myngconnect, Spelling City, ConnectEd, Prodigy (math review program), iReady, Brain Pop Jr., Epic and Storyline Online.

4th Grade: Class Dojo, McGraw Hill ConnectEd for Math and Reading, Spelling City, various math and language arts apps, Google Docs, Slides, Forms, Mail, Google Classroom, Brain Pop, Jr., Spelling City

5th Grade: Class Dojo, Google Classroom, Google Drive, Schoology, keyboarding sites, Class Dojo, Readworks.org, Biblionasium (reading tracker), Khan Academy, ABCYa.com, Prodigy, Utah Compose, Google Earth, ActivInspire, Microsoft PowerPoint, NitroTye, Ztype

• What supervision practices are in place when students are online?

Preschool: iPads are locked when students are using them to prevent distraction and straying from what is expected; iPads are used in the center next to the teacher during center time

Kindergarten: Students are locked into an app when using the iPad; aides help to monitor students while on iPads and logging into the chromebooks for Lexia.

1st Grade: Between 1 to 3 adults are in the room when students are on an iPad. Most first grade teachers have students use iPads and/or Chromebooks for only 12 to 15 minutes during center time.

2nd Grade: Teachers, parent volunteers, and students monitor each other in the classroom

3rd Grade: Teachers monitor technology use by walking around the room to check student Chromebooks and iPads; training in all classes about the appropriate use of technology; training to all students to let an adult know if any students are into sites they should not be in; Pear Deck during reading instruction allows for the teacher to monitor every device using the teacher iPad.

4th Grade: Students must be at desks, teacher monitors by walking around and assuring students are on the correct site(s)

5th Grade: Teachers are constantly monitoring around the classroom, and all screens can be visualized by teachers; Chromebooks are used only at student desks

• Are there management tools used that allow teachers to digitally monitor student use or limit access to some applications or sites?

-The firewalls we have are the initial safety tool that restricts and blocks websites and services that have no educational value to students. These firewalls are updated constantly to correct any issues that come.

- iPads are configurable to allow the teachers to restrict different services on the device, and we now have a Mobile Device Management that allows us to control and view different actions done on the iPads.

-We are currently transitioning from using LANSchool to monitor and control computer lab stations to Impero which will grant us more intuitive solutions for monitoring as well as even more features and options.

• What are the school rules when inappropriate information appears for students, staff and parents? Are there safe reporting procedures for students, staff, and parents so that reporting is safe and encouraged, when it happens?

-There is a 'bullying' link on our school website where students can safely report anything they feel falls into the cyber-bullying. (All bullying can be reported there; answer specific to internet and online.)
-Any violations are immediately reported to the principal. Any suspicion of inappropriate use may constitute the principal to contact the technology experts at the district. The principal handles each situation on an individual basis. The parent is always contacted and the principal holds a meeting with the parent(s) and student. Consequences *might include* limited use or forfeit of technology privileges and contacting the School Resource Officer.

• How does the school balance access and safety appropriate for the grade levels at your school?

-Students are given explicit instructions as to how, when, and where to access content on the web. Teachers model explicitly what websites students are allowed to access. Teachers also ensure that Chromebooks and devices are used only at students' desks or approved areas around the room, for specific purposes, and teachers constantly walk around and monitor student use.
-Weekly PLC discussions allow for continual communication between administration and staff regarding policies, procedures, and content with respect to each grade level.

• What does the administration see as important opportunities for our students related to constructive, proactive technology use?

-Access to technology devices
-Quality instruction and training for proper technology usage
-Ongoing training for teachers, students, and parents
-Unique opportunities such as Hour of Code
-Real world research
-Instructional content
-Skills practice
-Keyboarding
-Word processing
-App usage
-Overall computer skills

• What does the administration see as their greatest threats for your students?

-Accessing inappropriate content
-How students are using personal and/or school devices
-Inability to control the impact of mass media (social media, 24/7 news, fake news, etc.)

• What are the policies in place for devices brought from home – tablets, cell phones, etc.?

We do not currently allow any electronic devices from home to be used in the classroom. This includes no tablets, no cell phones, no Kindles, no iPads, etc.

• What does the administration see as the greatest threats for our students on the internet or online?

Lack of Education: Students have a lack of education to protect themselves in the online world. We as the school can only do so much. Filters can only keep so much out of view. The most effective way to keep students safe online is not to trust a filter alone, but to be completely involved in a child's internet world, to keep technology devices in full view and not in secret, to explicitly teach a child what

is appropriate and what is inappropriate and what to do if they come across something that makes them feel scared, threatened, uncomfortable, etc.

Supervision at Home: We have no idea what parental controls or monitoring procedures are in place in the student homes.

Supervision at School: Even with active monitoring around a classroom, a teacher is only one set of eyes. There are apps and websites that 'look' like a student is doing one thing when in reality, it is a cover for something else going on. When students are on electronic devices, screens are in full view and teachers are actively monitoring around the room to ensure proper usage.

Pop-ups: These can especially be a problem in free apps that are used. Our frustration is that we wish someone's job would be to help us keep the iPads manageable, delete stuff we don't use, and install or show us how to keep students from accessing other sites.

Off-task Behavior: Students know more about technology than some adults. Some students can get pretty sneaky about their computers. Many students also know how to delete the history, but there is a management system through Google where we can still retrieve it.

Filters: Filters only catch so much. The internet world is getting better at going around filters.

Inability to Always Control Content Being Searched: As teachers and staff, we try to closely monitor all times that a student is working on an internet device. With between 23-29 students per classroom, we do the best we can to see all students, but we do miss things. Students could have a few minutes to search anything they choose until the teacher might be back around to their area to monitor.

• **Explanation of training currently provided:**

• **To students about digital citizenship and safe use of technology?**

Every teacher trains students on appropriate usage of technology and the internet in their own classrooms. Our computer lab aide works through the district's advised internet safety training with the students the first couple weeks of school, when the students come to their regularly assigned computer time. No student gets on a computer at the beginning of each year without these trainings. Our computer lab aide also reviews the trainings during each trimester as reminders for students that have already been here, but also as new training for new students that have moved in. In the computer lab, the aide uses NetSafe Utah videos and discuss their application in detail.

K-3 topics include:

- The internet is not the real world.
- Be kind online, just like in real life.
- Don't give out any personal information to someone you don't trust and know in real life.
- Tell an adult you trust if anything happens that makes you feel sad, uncomfortable, or scared.

4-5 topics (in addition to the above) include:

- What to do about cyberbullying.
- How and why to be careful posting pictures online.
- How and why to be careful making friends online, in general do not befriend someone online that you don't know in real life.

Later in the year, we review these same topics using other videos/songs, etc. with discussion. And of course, we have a discussion on the spot anytime a kid has a question or something happens that provides a good teaching opportunity.

- **Explanation of training currently provided:**

- **To parents and guardians about how to discuss and support digital citizenship and safe technology use with their children and how to report inappropriate content?**

Our computer lab aide made a handout for kids to take home and discuss with their parents and display by their home computer. Trainings on this handout and internet safety expectations take place by the computer lab aide with students as they come to computer the first week in each trimester.

Updates: 3-14-17

***In response to questions asked in the 2-28-17 Community Council meeting, here is updated information:**

Questions: Why do students receive their own email address? When do you assign students an email? Why aren't parents notified they have an email address? How are students using the email addresses? How are we ensuring students are protected from predators and outside sources while having their own email address?

District Response:

We use Google for authentication to many applications. In order for this to work we must issue each student in the district a Google account. The account does include an email address, unlimited cloud storage, access to Google drive and other Google for Education products.

It is up to the schools to manage parent notification on all issues relevant to what is going on in the school. Notifying parents would fall under the Community Council responsibility.

Email addresses are used for authentication to Chromebooks, the G Suite, and other applications. Schools may choose to decide whether or not students can actually use the email account for sending email. Email can also be used for many types of classroom projects where students may have foreign pen pals, contact experts in specific fields and for general communication. Using email is a life skill, and we do teach proper use of internet provided services in the internet safety training programs we provide to the lab aides.

Google is a secure email system. Email safety is something we must teach our students, because safe use of the internet and email is dependent on how students use it. Just like we teach students to use crosswalks, look both ways when crossing the street, stranger danger, and all the other safe practices we teach children, the safe use of the internet (and email) must be taught. Google email addresses are protected data as defined by FERPA and CIPA. Email addresses are never distributed or given out by Google or the district."

Updates: 11-16-18

***In response to questions asked in the 10-23-18 Community Council meeting, here is updated information:**

Questions: What is my child's email? What is the username and password or how do I find that out? What does my child do with this email?

Response:

All students Kindergarten through 5th grade have a Washington County School District username and password that they use to access school resources like: School computers, Power School, Unified Classroom, iReady, Waterford, Imagine Learning, Spelling City, Google Classroom, and other individual grade-level software choices are used for this purpose.

Students usually know their username and password. As parents, you are welcome to that information. We suggest that you start by asking your child their username and password. If they do not know it or if they are unwilling to give it to you, then we would be happy to assist you at the school. Make sure to bring your ID with you so we can validate your identity, and then the school staff will give you access to that information. If the child has changed his/her username and password, then the school can reset it back to the default password, but then you will need to work with your child to change the password to something you both know.

In our school, we are very clear about the rules of using technology and it is reviewed a minimum of three times each year. Students are aware of what is appropriate use of their devices. Periodically, a very small amount of time, we will see students email their friends/classmates. We handle these on a one-on-one basis and the parent is contacted. The consequence is usually a loss of using the device for a period of time. When a student loses access to the device, we work with him/her to remind and teach appropriate school device use and behaviors with the intent to help them learn appropriate school digital use and regain access to school tools and resources.