

Keeping our Students Safe Online H.B. 213

Alpine School District has adopted a vision of technology use around seven integrated gears that work together to help students learn. Online Safety and security is an important part of our model. To learn more about our model [click here](#).

HB 213 has asked community councils to play a more active role in this important work. [Click here for state information about Community Council responsibilities](#). This is a report to help Community Councils in their new responsibilities. It is organized around three areas of responsibility: technology use, student education, and parent education.



Technology Use in School- Filtering, Management, and Supervision

Filtering Information

- Alpine School District uses the UEN recommended iBoss content filtering system with the recommended K-12 configuration.
- We have different rule sets for elementary and secondary schools so that we can allow some sites in secondary schools without allowing them for elementary schools, although most blocked sites are blocked on all student and guest networks.
- In our elementary computer labs we have a special login for K-2 users which limits use to the sites directed by the teacher and restricts search engines. We cannot enable unique settings for each school to maintain their own list of allowed and blocked sites. Besides the technological and bandwidth resources this would take, more complexity causes more vulnerability in any security environment.
- The filter works by categorizing known internet content and then allowing us to block inappropriate categories such as pornography, social networking, gambling, weapons, adult content, gaming, etc. Many sites are uncategorized and are blocked on the student network. Secondly, the filter has a list of keywords that will create a block if used in searching or if the keyword is in the internet address.
- ASD has three different networks: staff (district or school owned staff devices), student (district or school owned student devices), and guest (all personal devices) network. The guest network has the same rule set as the student network.
- iPads - Last year to close a vulnerability with iPads and our old filter, we used the Mobicip browser on our iPads in many settings. This vulnerability has been fixed with our new iBoss filter. If you would like to continue to use Mobicip for additional security and management, please contact Technology. It will cost between \$4 and \$6 a device per year. Mobicip has extended our trial for 30 days so you can compare Mobicip to the installed browser.
- You-Tube and Social Media sites like Facebook and Twitter - These sites are open on the staff network and closed on all other networks. The only exception is for the high school Social Media class where they are opened just within the lab under supervision of the instructor.
- Google Images - Google images are allowed for users as part of Google. Our iBoss filter has enabled safe search for image searches.
- Weebly and Blogspot Pages - By default these sites are open for staff but closed for students and guests. We open individual sites for teachers who create class websites in these platforms. These sites are not allowed for students to create individual sites and blogs for school use. The district provides a managed blogging service called edublogs for student and teacher blogs and sites using the asdpages.org domain. Google Sites is also available.

Management Systems

- Desktop and Laptop - The Alpine School District currently is using a site license for LanSchool to manage some desktop and laptop devices. This allows the instructor to monitor the screens of users electronically as well as lock down certain screens.
- Google Apps Management - We are also heavily integrated with Chrome Management for the many ChromeBook and ChromeBox devices that are in use today. It allows us to manage what apps and service are available for users. For instance, this system is what allows us to set our student gmails to send and receive email only to teachers and other students.
- MDM - We are in the process of configuring a MDM (Mobile Device Management) system to give us more management of other mobile devices, especially iPads. This will allow teachers to have some visibility and control of student iPads while in use.

Supervision

- Teachers are asked to monitor students whenever they are online, either electronically or by walking around the classroom.
- Teachers should never put a student on a device with access to the internet in a place or situation where the student knows that the teacher cannot monitor their activity such as in a hallway or back corner of the room.
- Teachers should take special care when directing students to add art or photos to projects by directing them to safe collections of picture and art like kidzsearch or kids.nationalgeographic.com.
- When inappropriate content is accessed by a student or staff member (either seemingly by accident or on-purpose), the student or students should be removed from the dangerous situation and the school principal or administration should be notified. The device should be isolated and the Technology Office should be contacted. Beside working to fix any issue discovered, the Technology Office will work with the administration to gather information and take appropriate measures if the Acceptable Use Policy was violated.

What can the Community Council do?

- Ensure that K-2 students use the K-2 login and all other students use their unique login with their unique password.
- Ensure that student created web pages are made through the supported asdpages.org or Google Sites.
- Make sure the filtering is working on all school devices by assigning someone to test student devices on the student network.
- Learn what management systems are at use in your school and when it may be helpful for teachers to use them.
- Learn about and help develop school based practices and procedures to ensure student safety online.
- Provide resources for online supervision where needed.
- Make sure information is communicated to the staff on how to respond if inappropriate content is accessed.
- Review the following [presentation](#) for possible teacher training.

Student Education

Elementary Schools

Digital Citizenship is one of the standards for our elementary technology specialist teachers. You can see the many [resources they have developed here](#). They include resources from NetSmartz, CommonSense media and other state and national resources.

- All teachers who go online should include digital citizenship as part of their regular instruction. The technology specialist is a great resource.

7th - 8th Grade

- Our Junior High Media teacher librarians have developed wonderful materials to help students develop digital citizenship skills that can be delivered as students rotate by class into the media center for an orientation.
- Specialty classes that use computers are great places for digital citizenship to be taught. These include Introduction to College and Career Readiness as well as Business and CTE classes.

9 - 12 Grade

- Each student is required to complete Computer Technology for high school graduation. This course includes standards specifically addressing digital citizenship topics. You can review the [course standards here](#).
- Many other high school courses include the use of technology and present many opportunities to develop digital citizenship skills.

What can the Community Council do?

- Develop a plan to specifically address digital citizenship in your school. Learn from the elementary technology specialist teacher, teacher librarian, and/or computer teachers in your school what their current practice is and what topics they cover with which students. It would be wise to invite these specialists to your meeting when you discuss this.
- Decide how you might share resources with other teachers to incorporate digital citizenship into their classes as they use online resources.
- Decide if you would like to sponsor a school-wide initiative to increase awareness around these practices or issues.

Parent Education

- Many organizations provide great information for parents to help students stay safe when online at home. A few great resources are:
utahpta.org/netsafety netsafeutah.org/ utahnetsmartz.org/
- Has your school provided any information or resources to parents in the past concerning online safety practices and tools?
- Has your school provided any information to parent concerning the topics and information their students receive concerning digital citizenship?

What can the Community Council do?

- Decide how you may best share resources for digital citizenship and online safety with parents. Consider the role of the community council to provide options and resources without being prescriptive and compulsory. This may include newsletters and other communications, back to school nights, parent conferences, carnivals, and other school events.

School Report

Inventory - Here is a breakdown of the number of devices students have access to at Cedar Ridge Elementary:

Type of Device	Quantity in School	Primary Use
iMac desktop	84	Student work and testing
Chromebook	191	Student work and testing
Kindle tablet	13	Student work
iPads	159	Teacher work and student work
Macbook laptop	20	Student work

Management - We use programs called LanSchool and Apple Remote Desktop to manage the devices the students use in the computer labs. These programs allow the teacher to remotely monitor what students are accessing on the computers. The principal manages the restrictions and apps on the iPads. Students in Grades K-2 are given minimal access to Internet sites. Students in Grades 3-6 must use their unique logins to use the computers. The logins are kept secure and students are taught to safeguard their login information. These logins would allow us to identify any individual who accessed inappropriate content at school. Student email accounts cannot receive emails from people outside of the Alpine School District network.

Supervision - Teachers know they must monitor the devices when they are being used with students. Students are trained to let the teacher know immediately if anything they come across makes them feel uncomfortable. Students are never allowed to use a device without adult supervision.

Digital Citizenship Plan - Students have Computers as a Specialty for about 5 weeks at a time, three times a year. Each year we have the whole school participate in a NetSmartz assembly about being safe online. Students are not only taught about being safe online, but also important lessons about not becoming a cyberbully. In addition to Computers Specialty, our school is working toward obtaining 500 mobile devices to increase student proficiency with technology.

Parent Resources and Information - For a list of resources, the skills taught, and commonly used websites in Computers Specialty, go to <http://cedarridge.alpineschools.org/digital-citizenship/>.

Policies - Students are not allowed to use devices brought from home without their teachers' permission.

Decision Making - Students in the lower grades are given much less access to the Internet. Students in Grades K-2 only use iPads and Kindles except when they are in the computer lab. Students in Grades 3-6 have access to Chromebooks and laptops but must use a unique login for these devices.

Guiding Principles - Our school is focused on preparing our students to be productive citizens in the 21st Century. Students need to learn how to be creative, solve problems, communicate, and collaborate with others--the proper use of technology helps us accomplish these goals. Our students also need to learn how to best use the resources available to them while being protected from exposure to harmful content.

This information is a general explanation of how devices are used at Cedar Ridge Elementary School. For detailed information for your child, please contact his or her teacher. Please contact the principal if you have any questions. Thank you.

A digital copy of this document can be found at <http://cedarridge.alpineschools.org/digital-citizenship/>.