Acceptable Use Policy (AUP)

Hoonah city School District's, HCSD, Acceptable Use Policy

For the use of Computers, Mobile Devices, Internet Access, Google Apps for Education Suite, and Internet Applications

Definitions

User includes anyone, including employees, students, and guests, HCSD technology, including, but not limited to, computers, networks, Internet, email, chat rooms and other forms of technology services and products.

Network is wired and wireless technology networks including school networks, cellular networks, commercial, community or home-based wireless networks accessible to students.

Equipment are cellular phones, 'Blackberry' [smartphone] type devices, PDAs, MP3 players, iPod type devices, and portable computers such as laptops, iPads, desktops, tablets and netbooks, as well as portable storage devices.

Technology provides students with unique and powerful ways to enhance their learning. The Hoonah City School District, HCSD, supports the use of technology for the purpose of enhancing and supporting learning and is pleased to offer Users access to computer networks so that they can access school-supplied technology to enhance learning any time of day.

It is one of the technology goals of the school to ensure that each User's interactions with technology contribute positively to the learning environment both at school and in the community. Negative use of technology through HCSD-owned devices inside or outside of our schools that degrades or defames other Users, or members of our community is unacceptable. The HCSD also recognizes that Users have widespread access to both technology and the Internet; therefore, use of personal devices and connectivity is considered to be included in this Acceptable Use Policy (AUP).

Access to HCSD's network is a privilege, not a right. The use of technology whether owned by HCSD or devices supplied by the Users entails personal responsibility. It is expected that Users will comply with HCSD rules, act in a responsible manner, and will honor the terms and conditions set by the school, and HCSD. Failure to comply with such terms and conditions may result in temporary or permanent loss of access as well as other disciplinary or legal action as necessary. In particular, students will be held accountable for their actions and are encouraged to report any accidental use immediately to their teacher or school administration.

With the increased usage of free educational applications on the Internet, digital storage areas, containing less sensitive User information, may or may not be located on property of the school or HCSD. In some cases, data will not be stored on local servers. Therefore, Users should not expect that files and communication are private. The HCSD reserves the right to monitor Users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of HCSD property, network and/or Internet access or files, including email. Google Apps in Educational Applications HCSD is offering Users a free educational suite of applications for use to enhance teaching and learning. Google Apps is a concept known as “cloud computing” where services and storage are provided over the Internet.

The HCSD is providing Users GoGuardian Security. This service provides System Administrators the capability to limit messages based on where they are from, where they are going, or the content they contain. The HCSD will use this technology protection measure to block or filter, to the extent practicable, access of visual depictions that are obscene, pornographic, and harmful to minors over the network.

In order for Users to gain access to Gmail and his/her Educational Google Applications account on the Internet, the HCSD must obtain parental permission for a minor under the age of 18 years. Students 18 years and older are also required to acknowledge and accept HCSD’s terms and conditions prior to obtaining access to technology within our schools.

Terms and Conditions

These are examples of inappropriate activity on the HCSD network, but HCSD reserves the right to take immediate action regarding activities

> 1) that create security and/or safety issues for the HCSD network, Users, schools, network or computer resources;
>
> 2) that expend HCSD resources on content it determines lacks legitimate educational content/purpose; or
>
> 3) other activities as determined by HCSD as inappropriate.
>
> > 1. Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
>
> 4. Criminal activities that can be punished under law.
>
> > 1. Selling or purchasing illegal items or substances.
> >
> > 2. Obtaining and/or using anonymous email sites, spamming, spreading viruses.
> >
> > 3. Causing harm to others or damage to their property.
> >
> > 4. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
> >
> > 5. Deleting, copying, modifying, or forging other Users’ names, emails, files or data, disguising one’s identity, impersonating other users, or sending anonymous email.

6. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.

7. Using any HCSD computer/mobile devices to pursue “hacking,” internal or external to HCSD, or attempting to access information protected by privacy laws.

8. Accessing, transmitting or downloading large files, including “chain letters” or any type of “pyramid schemes.”

9. Using web sites, email, networks, or other technology for political uses or personal gain.

10. The HCSD internet and intranet property must not be used for personal benefit.

13. Users must not intentionally access, create, store or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.

11. Advertising, promoting non-HCSD sites or commercial efforts and events

12. Users must adhere to all copyright laws. Users are not permitted to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Code of Student Conduct.

13. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors.

14. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school system technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.

15. Users may not create or introduce games, network communications programs or any foreign program or software onto any school system computer, electronic device or network without the express permission of the technology director or designee.

16. Teachers shall make reasonable efforts to supervise students’ use of the Internet during instructional time.

Cyber safety and Cyberbullying

All Users - Despite every effort for supervision and filtering, all Users and Students' parents/guardians are advised that access to the network may include the potential for access to content deemed inappropriate. Every User must take responsibility for his or her use of the network and make every effort to avoid those types of content. Every User must report security or network problems to a teacher, administrator, or system administrator.

Personal Safety – In using the network and Internet, Users should not reveal personal information such as home address or telephone number.

Confidentiality of User Information – Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.Active Restriction Measures – the HCSD will utilize filtering software or other technologies to prevent Users from accessing visual depictions that are

(1) obscene,

(2) pornographic, or

(3) harmful to minors.

Attempts to circumvent or 'get around' the content filter are strictly prohibited, and will be considered a violation of this policy. The HCSD will also monitor the online activities of Users through direct observation and/or other technological means.

Interactive Web 2.0 Tools

Technology provides an abundance of opportunities for Users to utilize interactive tools and sites on public websites that benefit learning, communication, and social interaction.

Users may be held accountable for the use of and information posted on these sites if it detrimentally affects the welfare of individual users or the governance, climate, or effectiveness of the school(s). From time to time, teachers may recommend and use public interactive sites that, to the best of their knowledge are legitimate and safe. As the site is "public" and the teacher, school, and HCSD is not in control of it, all Users must use their discretion when accessing information, storing, and displaying work on the site. All terms and conditions provisions in this AUP also apply to User-owned devices utilizing the HCSD network.

Student Use of Interactive Web 2.0 Tools

Online communication is critical to the students' learning of 21st Century skills, and tools such as blogging, podcasting, and chatting offer an authentic, real-world vehicle for student expression. Student safety is the primary responsibility of teachers.

Therefore, teachers need to ensure the use of Google Documents, classroom blogs, student email, podcast projects, email chat features, or other Web interactive tools follow all established

Internet safety guidelines including:

- The use of Docs, blogs, podcasts or other web 2.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web 2.0 tools. This includes—but is not limited to—profanity, racist, sexist, or discriminatory remarks.

- Students using Docs, blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts.

- Students should NEVER post personal information on the web (including, but not limited to, last names, personal details such as address or phone numbers, or photographs).

- Students should NEVER, under any circumstances, agree to meet someone they have met over the Internet.

- Any personal blog a student creates in class is directly linked to the class blog which is typically linked to the student profile and therefore must follow these blogging guidelines. In addition to following the information above about not sharing too much personal information (in the profile or in any posts/comments made), students need to realize that anywhere they use the blog login it links back to the class blog. Therefore, anywhere that login is used (posting to a separate personal blog, commenting on someone else's blog, etc.), the account should be treated the same as a school blog and should follow these guidelines.

- Students should never link to web sites from their blog or blog comments without reading the entire article to make sure it is appropriate.

- Students using such tools agree to not share their user name or password with anyone besides their teachers and parents and treat Web posting spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog.

- Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

Student Use of Mobile Devices

- The HCSD has provided some students with Chromebooks for use both in school as well as away from school. The HCSD-owned devices follow the stipulations outlined in this AUP as well as a specific device Responsible Use Agreement, RUA.

- School Administration and HCSD Technology staff may search the student's memory device if they feel school rules have been violated, which may include, but are not limited to, audio and video recording, photographs taken on school property that violate the privacy of others, or other issues regarding bullying, etc.

- Students may not use an audio recording device, video camera, or camera (or any device with one of these, e.g. cell phone, laptop, tablet, etc.) to record media or take photos during school unless they have permission from both a staff member and those whom they are recording.

- These rules apply to student-owned devices as well. A student-owned mobile device is a non-HCSD supplied device used while at school or during school activities. The students may use the student-owned mobile devices in class only with the teacher's expressed permission.

Student Supervision and Security

The HCSD does provide content filtering controls for student access to the Internet using HCSD's network as well as reasonable adult supervision, but at times inappropriate, objectionable, and/or offensive material may circumvent the filter as well as the supervision and be viewed by students. Students are to report the occurrence to their teacher or the nearest supervisor. Students will be held accountable for any deliberate attempt to circumvent HCSD technology security and supervision.

Students using mobile and cellular devices while at school, during school or HCSD-sponsored activities are subject to the terms and conditions outlined in this document and are accountable for their use.

Please note that this document is subject to change without notice.

Hoonah City School District
366 Garteeni Highway
Hoonah, Alaska 99829
907.945-3613

Student Name (Print)　　Phone Number　　Email Address

(Signature)　　Date:

Advisory Teacher　(Print)　　Phone Number　　Email Address

(Signature)　　Date:

Technology Acceptable Use Acknowledgment Form

Name of Employee	
Position	
School Year	
Date of Birth*	

~I have read the Hoonah City Schools' acceptable use agreement referenced in the title of this document. _______ (initial)

~I agree to follow this policy and its regulations. _______ (initial)

~I further understand that if I violate this policy, I will face disciplinary action in accordance with Hoonah City Schools' policies along with state and federal laws. _______ (initial)

~I hereby release the members of the Hoonah City School Board of Education, their officers, employees, agents, representatives, and affiliates, from any and all claims and damages of any nature arising from my misuse or inability to appropriately use, the school system's electronic information systems and educational technology resources. The Hoonah City Schools is not liable for any claims that may arise from my use of the system's computer information systems and educational technology resources to purchase unauthorized products and/or services. _______ (initial)

Signature of Employee	
Date Signed	
Personal Email Address	