Technology Appropriate Use Guidelines
Oakridge School District
January 2015

Purpose of Technology Appropriate Use Guidelines

District owned technology is to be used to enhance learning and teaching as well as improve the operation of the district. Technology, as referred to in these guidelines, is any electronic device that is used by students or staff.

The Oakridge School District's electronic communications network, OSD Network, is to be used to support and enhance learning and teaching that prepares students for success. Providing access to OSD Network is an investment in the future of both our students and staff. OSD Network supports the core beliefs of the Oakridge School District:

- Do what's best for students.
- Continue to learn and grow.
- Respect and care about each other.

The Oakridge School District believes that electronic communication is a tool for lifelong learning, and that access to OSD Network is one of the resources that promote educational and organizational excellence. We believe the responsible use of OSD Network and 21st Century equipment will propel today's schools into the information age. These tools and resources will allow students and staff to significantly expand their knowledge by accessing information resources as well as analyzing, synthesizing, and publishing information.

Students and staff are expected to use OSD Network in a responsible, efficient, ethical, and legal manner in accordance with the mission of the Oakridge School District. The use of OSD Network is a privilege, not a right, which may be revoked at any time for inappropriate behavior. Users assume responsibility for understanding relevant board policy and these guidelines as a condition of using OSD Network. Staff members are accountable to teach and use OSD Network responsibly. Use of OSD Network that is inconsistent with policy and guidelines may result in loss of access as well as other disciplinary or legal action.

The purpose of this document is to provide guidance to students and staff in the use of technology in order to maximize the derived benefits, provide safety in the use of technology, and insure the security of confidential information.

Related Laws and Board Policies

Federal Laws

CIPA -The Children's Internet Protection Act is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers.

What CIPA requires: Schools and libraries subject to CIPA may not receive the discounts offered by the E-Rate program unless they certify that they have an Internet safety policy and technology protection measures in place. An Internet safety policy must include technology protection measures to block or filter Internet access to pictures that: (a) are obscene, (b) are child pornography, or (c) are harmful to minors, on computers (including mobile devices) that access the Internet by minors.

Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors; and Schools and libraries subject to CIPA are required to adopt and implement a policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) restricting minors' access to materials harmful to them.

Schools and libraries are required to certify that they have their safety policies and technology protection in place before receiving E-Rate funding.

CIPA does not affect E-Rate funding for schools and libraries receiving discounts only for telecommunications, such as telephone service.

An authorized person may disable the blocking or filtering measure during any use by an adult to enable access for bona fide research or other lawful purposes.

CIPA does not require the tracking of lnternet use by minors or adults.

FER_ PA- Family Educational Rights and Privacy Act- A Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records and specifies how districts should handle requests for student information.

HIPAA-Health Insurance Portability and Accountability Act of 1996 -A federal law to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addressed the security and privacy of health data.

State Laws

ORS 244.040 - Prohibited use of official position or office; exceptions; other prohibited actions

ORS 260.432 Campaign Finance-The restrictions imposed by the law of the State of Oregon on your political activities are that "No public employee shall solicit any money, influence, service or other thing of value or otherwise promote or oppose any political committee or promote or oppose the nomination or election of a candidate, the gathering of signatures on an initiative, referendum or recall petition, the adoption of a measure or the recall of a public office holder while on the job during working hours. However, this section does not restrict the right of a public employee to express personal political views."

Oakridge SD Board Policies

Board Policy 160.2 -Use of District Property-This policy directs that no Oakridge property will be removed from or used by any person(s) or organization(s) without the written consent of the building administrator. This document will extend authorization to the Technology Coordinator as well.

Board Policy 363- Personal Electronic Devices and Social Media- Staff. This policy identifies acceptable use of social media for staff and provides guidance of electronic communication with students during and after school hours.

Board Policy 343- Electronic Communication-Information Systems. This policy describes system use, system access, security, personal security, copyright and general use definitions and proceedures.

Board Policy 345- Appropriate Use Policy for Computers and Internet Access. This policy specifies requirements for obtaining access for students and give an overview of limitations and responsibilities of the student.

Definitions

OSD Network	Oakridge School District's electronic communications network connects all school sites together with Internet access.
District Oakridge Email	Student and staff email accounts provided by the district.
Filtering	A process to deny access to certain websites or resources as defined in the filter.
Internet	A worldwide network that connects smaller networks together.
Social Networking	Websites that provide means of personal communications between participants (i.e. FaceBook, MySpace)
iPortai (Moodie)	An open source course management system available to teachers, staff, and students.
Wiki	"A website that allows the easy collaborative creation and editing of any number of interlinked web pages via a web browser using a simplified markup language or a WYSIWYG text editor."-Wikipedia definition http://en.wikiQedia.org/wiki/Wiki - cite note-0
Blog	Blend of the terms web and log. It is considered a type ofwebsite. Blogs are usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video.

Student Safety and Privacy Guidelines

General Guidelines

The Oakridge School District has an obligation to protect student safety and to balance this with the need for open communications when using the Internet. There are documented instances of students being inappropriately identified via the Internet and thereby becoming subjected to unhealthy situations or unwelcome communications.

The purposes of these guidelines are:

- To inform school staff of the possible dangers of allowing students to publish identifying information on the Internet;
- To recognize that there are potential advantages of allowing students to publish identifying information on the Internet; and
- To provide to schools a recommended set of Guidelines governing how student-identifying information should be allowed in publishing on the Internet.

Staff and student users of OSD Network must be aware that information accessed, created, sent, received, or stored on the network is not private. It is subject to review by network system administrators, lawyers, and others who may investigate complaints regarding inappropriate or illegal material.

ALL K-12 Students

It is clear that there are significant risks, as well as significant advantages, involved with allowing students to be identified on the Internet. Therefore students should not be easily identifiable from materials they might publish on the Internet. No directory information should be posted on the web for students whose parents have returned the form asking that such information not be released.

Student Internet Publishing Guidelines

- Only first names should be used in published student work.
- Pictures that are a part of student publishing should not include identifying information.
- Under no circumstances should a student's home address or phone number be included.
- If replies to published student work are appropriate, the sponsoring teacher's address should be the email address displayed, not the student's.
- In special circumstances with parent-signed release, identifying information can be added.
- No social sites are to be accessed using District provided student email accounts.

Additional High School Guidelines

Interactive Online Forms and Applications

There are circumstances where it may be appropriate for older students (Grades 9-12) to provide identifying information along with work published on the Internet. The OSD recognizes that high school student publications on the Internet may allow more identifying information where it is considered appropriate by the student, parent, and the supervising staff member.One example might be college entrance or employment opportunities that would be enhanced by viewing a student's work on the Internet. To make this determination the submitting high school student and the supervising staff member must carefully weigh the

potential for risk against the perceived advantage of providing this identifying information. Students are required to seek guidance and approval from parents and school staff before providing identifying information. It is imperative that the site the students are communicating personal information to is a secure site- https.

Online Safety Resources

The websites below provide safety information for adults

and children. http://www.csriu.org/- Center for Safe and

Responsible Internet Use http://www.safekids.com/- General

Resource Site http://www.getnetwise.org/- Internet

Education Foundation http://www.wiredsafety.org- Wired

Safety

http: //www.missingkids.com/- National Center for Missing and Exploited Children

Use of District-Owned Technology Devices

General Guidelines

The purpose of district-owned technology resources is to enhance the educational experience of students and to increase the operational efficiency and teaching of staff. Practices that attempt to achieve this purpose in a safe, legal manner are acceptable while practices that do not attempt to achieve this purpose are unsafe or detrimental and are considered not acceptable.

Teachers, specialists, and other supervising adults will teach and discuss the appropriate use of OSD Network, technical resources, and the Internet with their students, monitor their use, and intervene if the resource is not being used appropriately. The District will provide training resources for staff and students to use in their buildings.

Internet users are encouraged to find resources, such as email, blogs, wikis, and websites that meet their individual needs and take advantage of the networks many useful functions. There are many applications that can be used in an educationally beneficial manner as well as applications that can be used in an inappropriate, illegal, or unacceptable manner. Therefore, the District has established an adaptive baseline of filtered websites across all K-12 schools and a bypass list is maintained for students in grades K-2. Additionally, individual school staffs in conjunction with the Technology Department may choose to filter additional sites beyond the District minimums.

Although the District has deployed an Internet filtering system and students are supervised when they use the Internet, this does not guarantee that students will not access inappropriate materials or sites that parents consider objectionable. Oakridge School District's guidelines for accessing the Internet prohibit access to material that is inappropriate in the school environment. Students should report inappropriate access of material to a teacher, other staff person, or their parents. Parents are encouraged to discuss responsible use of the Internet with their children at home and how this responsibility extends to using the Internet appropriately at school.

District equipment that is used off site is subject to the same rules as when used on site. However,

users should be aware that OSD Network filter does not work outside of the district network.

Unacceptable Use of OSD Network and Equipment

The Student Handbook govern student discipline. School Board Policy and District Administrative Rules govern staff use.

The unacceptable uses of OSD Network may result in suspension or revocation of network privileges. Unacceptable use is defined to include, but not be limited to, the following:

- Violation of School Board Policies, District Administrative Rules, or any provision in the district Student Handbook.
- Transmission of any material in violation of any local, state, or federal law. This includes, but is not limited to: copyrighted materials, threatening or obscene material, or material protected by trade secret.
- The use of profanity, obscenity, or other language that may be offensive to another user.
- Any form of vandalism, including but not limited to: damaging hardware, computer systems, or networks, and/or disrupting the operation of the network.
- Copying and/or downloading commercial software or other material e.g. music, in violation of federal copyright laws.
- Use of the network for financial gain, commercial activity, or illegal activity, e.g. hacking.
- Use of the network for political activity.
- Use of the network to access pornographic or obscene material.
- Creating and/or placing a computer virus on the network.
- Accessing another person's individual account. Passwords should never be shared with another person and should be changed frequently. Passwords should not be common words or names that can be found in a dictionary.
- Posting information or images that could be a form of harassment or could promote a negative culture in the school environment by causing a student or staff member to feel uncomfortable or unsafe at school
- Activity with a malicious intent to disrupt the network
- Installation of unapproved equipment e.g. wireless access points, routers, switches, network cabling not provided or approved by the Technology Department; unapproved or unlicensed software; or changing of district settings is prohibited. The potential for "hackers" into our network is breached by any of these activities.
- Bypassing of District specified filtered Internet websites on computers used by students.

Use of Personal Technology Devices at School

Staff Guidelines

Personal staff equipment brought to school for instructional purpose use is under the understanding that loss or damage of equipment is solely on the owner/user. All policies and guidlines apply to personal devices while in district buildings.

Acceptable Use of Personal Technology

Personal devices, such as cell phones, smart phones, tablets, digital cameras, MP3 players, and laptops may be used for instructional purposes in the classroom at the discretion of the teacher. The same personal devices may be used outside of the classroom at the discretion of the school. However use of OSD Network resources, such as email, chat, wikis, blogs, and Internet websites must be done in a responsible and respectful manner.

Some software publishers allow home use by staff according to the "80/20 Rule." This rule states that if a school purchases a software license for a specific computer where the teacher/staff is the primary user (80%+ of the time at school), the teacher/staff may install the software on a home computer at no extra charge. The use of the software at home is governed by the same license agreement as at school, (i.e., it may not be used for commercial/for-profit use.) The 80/20 Rule only applies to staff and

faculty, for as long as they are employed by the school district. Student computers do not qualify for the 80/20 rule.

Unacceptable Use of Personal Devices

Students and staff are encouraged to use district equipment whenever possible. Unacceptable use of personal technology devices by students may result in suspension or revocation of personal device privileges. These included, but are not limited to:

- Use of a personal device that violates any of the unacceptable uses for district-owned technology listed above.
- Use of a personal device to gain or give an advantage in a testing situation.
- Use of personal devices during class that are not approved by the school or the individual teacher (e.g. cell phones, smart phones, tablets, digital cameras, MP3 players, and laptops).
- Downloading and installing district licensed software on personal devices unless specifically allowed by the licensing agreement.

Network Communication Guidelines

General Guidelines and Netiquette

Users of email, chat, blogs, wikis, and other network services should understand that everything that they post is public for all to see. Email messages are not private. Once it is posted it can never truly be removed from the Internet. District technical staff has access to all mail in order to maintain the system. All email is archived for a period of three years, and is subject to public records requests. All FERPA, HIPA, CIPA, and COPPA protections would still apply to email before being disclosed. Users should be aware of the common netiquette that users expect from one another:

- When sending email, make your "subject" as descriptive as possible.
- Check your email frequently and handle it appropriately after reading it, i.e. file, delete.
- Be very careful who your message is addressed to and how you reply. Do not "Reply All" unless you really want everyone on the original message to see your reply.
- Use BCC (Blind Carbon Copy) instead of CC when sending to a large number of email addresses, such as parents, and include sending to yourself. In doing so, the recipients will not see the emails of all others that are being copied nor will they need to scroll through a long list of email addresses on a small mobile/handheld device.
- Both incoming and outgoing email is filtered for spam and is blocked or quarantined based on the source and content of the email. Not all spam will be caught by any filtering system.
- Do not post the personal addresses or phone numbers of students or colleagues.
- Proofread and edit messages before they are sent, but be tolerant of errors in messages from others.
- Be careful when using sarcasm and humor: without face-to-face communications, a joke may not be taken the way it was intended.
- All communication should be respectful and professionaL
- Protect the privacy of other people.
- Messages written in ALL CAPITALS are difficult to read and are the network equivalent of shouting.

- Manage the email resources that you are allocated in order to stay within the set data space quotas.

Staff Oakridge Email Accounts

All Oakridge staff members are issued an email account. Guest teachers, in general, are not issued email accounts. Long-term guest teachers are an exception. All Oakridge email users are expected to use commonly accepted practices. Retired personnel are removed 90 days after July 1 of the year of retirement unless specific exceptions are made for serving on Oakridge committees or be asked to conduct a specific Oakridge task.

Acceptable Use of Email Accounts

- Using email to fulfill the responsibilities of your assigned position.
- Communication in a professional manner with staff, students, parents, vendors, and the community.
- Incidental personal use during duty-free time.
- Creating Oakridge hosted web sites, wikis, blogs, and class management systems (Moodie) to facilitate the communication of class information.

Unacceptable Use of Email Accounts

- Violation of Oregon Law ORS 260 on political activity.
- Violation of Oregon Law, School Board Policy, District Administrative Rules, or any provision in the district Student Rights and Responsibilities Handbook.
- The use of vulgar and plainly offensive, obscene, or sexually explicit language in any form.
- Using your Oakridge email account to subscribe to personal web resources, i.e. Facebook, MySpace, eBay, Twitter, etc.
- Copying commercial software or other material in violation of federal copyright laws.
- Use of the network for financial gain, commercial activity, or illegal activity.
- Accessing another person's individual account i.e. guest teacher, student teacher...
- Sharing of inappropriate materials or their sources with students or adults or knowingly accessing inappropriate materials.

Student Oakridge Email Accounts

General Overview

All Oakridge students are issued an Oakridge Google email account. All Oakridge Email users are expected to use commonly accepted practices.

- High school and middle school students have their Oakridge email accounts activated automatically unless a parent or guardian has denied access at the building level or filled out a denial form at the district level. (Denial Form)

Staff Use of Social Networking Sites[1]

The district recognizes the value of student/teacher/parent interaction on educational networking sites (i.e. social networking sites dedicated to professional activity/collaboration/networking). Collaboration, resource sharing, and student/teacher, student/student, and teacher/parent dialog can all be facilitated by the use of networking tools. Such interactivity outside of the school walls can greatly enhance face to-face classes.

Since social networking is relatively new to many staff members, the following are guidelines for maintaining a clear line between personal social networking and professional/educational social networking. Both have a valued place in our increasingly digital lives.

Your Online Identity

As educators, we have a professional image to uphold, and how we conduct ourselves online impacts this image. As reported by the media, there have been instances of educators demonstrating unprofessional conduct while engaging in inappropriate dialogue about their schools and/or students, or posting pictures and videos of themselves engaged in inappropriate activity online. Mistakenly, some educators assume that being online shields them from having their personal lives examined. Online identities are public and can cause serious repercussions if behavior is careless. For a Oakridge professional teaching site, use your Oakridge email account.

Friending

One of the hallmarks of online networks, whether personal or professional, is the ability to "friend" others and thus create an online group that shares interests and personal news. Oakridge School District discourages staff members from accepting invitations to "friend" students within personal social networking sites. When students gain access into a staff member's network of friends and acquaintances and are able to view personal photos and communications, the student-teacher dynamic is altered. By "friending" current students, staff members provide more information than one should share in an educational setting.It is important to maintain a professional relationship with students to avoid relationships that could cause bias in the classroom. Social networking can be a way to stay connected with students after they have graduated, but even then staff members should use their best judgment when "friending"students who have graduated.

The potential for "friending" parents of students also exists and can create some awkwardness for educators who want to maintain a clear line between their private and professional lives. Those who find themselves in the delicate position of either "unfriending"parents who are already a part of their social network or of not accepting requests for friendship can use the following language to help them out: "Our district has provided us with guidelines to help us navigate the line between our personal and professional online activities.I use my Facebook account solely within the realm of my personal life and would like to maintain that personal/professional distinction. In the spirit of maintaining that distinction I need to not "friend" parents of students." The following are recommended practices.

Recommendations for Professional/Educational Social Networking by Staff

- Let your administrator, fellow teachers, staff, and parents know about your educational network.
- Use district-supported networking tools (e.g. Oakridge email account).
- Do not say or do anything using a site attached to your Oakridge account that you would not say or do as a teacher in the classroom. (Remember that all Oakridge online communications are archived.)
- Have a clear purpose and outcomes for the use of the networking tool, and establish a code of conduct for all network participants.
- Adhere to the district guidelines when posting student pictures and using student names. Use only student initials in an email. (see Acceptable Use Section)
- Pay close attention to the site's security settings and allow only approved participants access to the site.

Recommendations for Personal Social Networking by Staff

- Do not accept students as friends on personal social networking sites. Decline any student-initiated friend requests and do not initiate social networking friendships with students.
- Use your best judgment when "friending" former students AFTER they have graduated.
- Do not friend parents of students.
- Do not post to or update your page during work hours. Yes, you may be on your lunch break, but others who see your page may inaccurately infer that you are social networking when you should be teaching.
- Remember that people classified as "friends" have the ability to download and share your information with other people. You don't have control over others with whom they share your information.
- Post only what you want the world to see. Imagine your students, their parents, or your administrator visiting your site. It is not like posting something to your website or blog and then realizing that a story or photo should be taken down. Once you post something on a social networking site it may be accessible even after it is removed from the site.
- Check your profile's security and privacy settings. At a minimum, educators should have all privacy settings set to "only friends." "Friends of friends" and "Networks and Friends" open your content to a large group of unknown people. Your privacy and that of your family may be at risk.

Recommendations for All (Personal and Professional) Social Networking by Staff

- Do not use commentary deemed to be defamatory, obscene, proprietary, or libelous. Exercise caution with regards to exaggeration, colorful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterizations.
- Staff members receiving information on a social networking site that falls under the mandatory reporting guidelines, must report it as required by law.
- Stay informed and cautious in the use of all new networking technologies.

Resources

Should Students and Teachers be Online Friends? Cheri Lucas

http://www.education.com/magazine/article/Students Teachers_Social_Networking/

A Teachers Guide to Using Facebook, Bernadette Rego
http://www.scribd.com/doc/16957158/Teachers-Guide-to-Using-Facebook-Read-Fullscreen

Student Access to Third-Party "Under 13" Website Services (Google Apps for Education)

General Overview

- All Oakridge students under 13 years of age must have a "Google Apps for Education" consent form signed by a parent/guardian and their teacher. The goal is to allow students to use this very valuable tool while following the Google recommendations and staying compliant with COPPA.

- Once students have returned consent forms, Google Apps will remain accessible for the current school year. Use of Google Apps will be suspended at the end of each school year.

- Google Apps consent forms must be renewed at the beginning of each school year.

Schools using Google Apps Education Edition, assume the responsibility for complying with the Child Online Privacy Protection Act (COPPA) and the information that students submit. When offering these online services to children under 13, schools must be cognizant that COPPA is a regulation that requires parental consents for the online collection of information about users younger than 13. Per the Google Apps Education Edition Agreement, any school administering Google Apps Education Edition acknowledges and agrees that it is solely responsible for compliance with COPPA, including, but not limited to, obtaining parental consent concerning collection of students' personal information used in connection with the provisioning and use of the Services by the Customer and End Users. In Oakridge School District, parental notification and consent will take place in the form of a permission slip granting use of Google Apps for ALL Elementary and Middle school students. This form must be signed on a yearly basis and held on file in the school office.

Access to the Internet enables students to explore thousands of libraries, databases, and other resources. The District expects faculty to blend thoughtful use of the Internet throughout the curriculum and provide guidance and instruction to students in its use. Access to Internet resources will be structured in ways that point students to those evaluated prior to use. However, students will be able to move beyond those resources to others not previewed by staff. Outside of school, families bear responsibility for the same guidance of Internet usage as they exercise with other information services.

Students utilizing District provided Internet access must first have the permission of and must be supervised by Oakridge School District (OSD) professional staff. Students utilizing school-provided Internet access are responsible for good behavior on-line just as they are in a classroom or other area of the school. The same general rules for behavior and communications apply.

The purpose of District-provided Internet access is to facilitate communications in support of research education. OSD is currently employing the use of Google Apps for Education, which is an fully online collaborative tool and a way for all students to demonstrate mastery of National Education Technology Standards. What is Google Apps for Education?

- Google Apps is a web-based suite of programs (Google Calendar, Google Sites, Google Docs/Slides/Sheets, Google Mail, Groups and Classroom) provided free to Schools
- All staff and students in OSD have access to Google Apps.
- all of the Google Apps services can be accessed from any device, anywhere with an internet connection.
- Google Apps allows you to easily collaborate and share documents and projects with classmates and teachers, turn in assignments electronically and more.

Student email accounts via Google Apps

- Every OSD student is assigned a unique username when tye enroll in the District. It will be their username during their entire OSD Experience.
- Every OSD student is assigned a unique password
- Usernames and passwords can be used in any OSD facility for Google Apps

To remain eligible as users, students' use must be in support of and consistent with the educational objectives of the OSD. Access is a privilege, not a right. Users should not expect that files stored on school-based computers will be private. Electronic messages and files stored on school-based computers may be treated like school lockers. Administrators and faculty may review files and messages to maintain system integrity and insure that users are acting responsibly.

The intent of this agreement is to ensure that students will comply with all Network and Internet acceptable use policies approved by the District. In exchange for the use of the Network resources either at school or away from school, the student understands and agrees to the following:

1. The use of the Network is a privilege, which may be revoked by the District at any time and for any reason. Appropriate reasons for revoking privileges include, but are not limited to,

altering system software, placing unauthorized information, using District equipment for cyberbullying or other inappropriate uses, placing computer viruses or harmful programs on or through the computer and/or network.OSD reserves the right to log computer use, monitor file server space, remove files, limit or deny access, and refer the student for other disciplinary actions.

2. The District reserves all rights to any material stored in files and will remove any material which the district, at its sole discretion, believes may be unlawful, obscene, pornographic, abusive, or otherwise objectionable. Students will not use their District-approved computer account to obtain, view, download, or otherwise gain access to, distribute, or transmit such materials.
3. All information, services and features on District resources are intended for the private use of its registered users and any use of them for commercial-for-profit or other unauthorized purposes (i.e. advertisements, political lobbying) is expressly forbidden.
4. The District resources are intended for the exclusive use of their registered users. The student is responsible for use of his/her account and password and privileges. Any problems arising from the use of the student's account are the responsibility of the account holder. Use of an account by someone other than the registered account holder is forbidden and may be grounds for loss of access privileges.
5. Any misuse of the account will result in suspension of the account privileges and/or other disciplinary action determined by OSD. Misuse shall include, but not be limited to:
    a. Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users;
    b. Disrupting the operation of the Network, Internet, or any other computer system through abuse of or vandalizing, damaging, or disabling the hardware or software;
    c. Malicious use of the network through hate mail, harassment, profanity, vulgar statements, or discriminatory remarks;
    d. Interfering with others use of the network or accessing the materials, information, or files of another without their prior approval;
    e. Use for non-curriculum communication such as, but not limited to instant messaging and online chatting. Responding to unsolicited on-line contact is strictly prohibited for student safety;
    f. Unauthorized installation, downsizing, copying, or use of licensed or copyrighted software or plagiarizing materials;
    g. Misrepresenting others on the network or allowing anyone else to use an account other than the account holder;
    h. Accessing, uploading, downloading, or distributing pornographic, obscene, or sexually explicit material;
    i. Violating any local, state, or federal statute;

1. District and network resources are to be used exclusively for the support of the academic program, not for entertainment.
2. Students bringing data files into the system agree to check the file with a virus- detection program before opening the file for use. Should the student deliberately or maliciously infect the network with a virus or cause damage through other vandalism, the student will be liable for any and all repair costs to restore the network to full operation and will be subject to additional disciplinary measures.
3. The student may only log on and use the network under the immediate supervision of staff member and only with the student's authorized log-in.

Violation of district policies and rules will result in appropriate suspension of computer access to be determined by OSD staff. Additional disciplinary action will be determined at the building level in keeping with existing procedures and practices regarding inappropriate language or behavior. When or where applicable, law enforcement agencies may be involved.

The Oakridge School District makes no warranties of any kind, neither expressed nor implied, for the network/Internet access it is providing. The District will not be responsible for any damages users suffer, including-but not limited to-loss of data resulting from delays or interruptions of service. The District will not be responsible for the accuracy nature, or quality of information.

OSD will make all reasonable attempts to prevent inappropriate access to students' personal information through the Internet. The District's intent is to make Internet access available for educational goals and objectives. However, students may find ways to access other materials as well. Even though the District institutes technical methods or systems to regulate students' Internet access, these methods cannot guarantee compliance with the district's acceptable use policy. OSD believes that the benefits to students of access to the Internet exceed any disadvantages. The District is committed to helping students use the Internet responsibly, but it is not possible to monitor student usage at all times. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information. Therefore, OSD will provide parents and guardians the option of requesting for their minor children alternative activities not requiring Internet use.

Oakridge School District
Network and Internet Access Agreement for Students

I agree to abide by the rules and regulations of system usage provided by OSD and to those which may further be added from time to time by the district and will be provided to me at that time. These rules will also be available in hardcopy form in the principal's office.

_____ _____
Signature of Student Date

As the student's parent or legal guardian, I agree to his acceptance of OSD policies regarding network/Internet usage and agree to pay for any fees, expenses, or damages incurred as a result of my child's deliberate, illegal, or malicious use of or damage to the network. I understand that parental refusal to allow students to make use of the Internet does not prohibit students from taking part in state and locally mandated testing and evaluation on the computer or through the network.

_____ _____
Signature of Parent/Guardian Date

YES____ NO____ I give permission for my student to access their school email account and Google Apps for Education for this school year.

_____ _____
Signature of Parent/Guardian Date

Copyright & Plagiarism

General Guidelines

Adherence to federal copyright law is required in both print and electronic environments. School Oakridge District Oakridge Administrative guidelines states District intent to adhere to the provisions of Public Law 94-553 and subsequent federal legislation and guidelines related to the duplication and/or use of copyrighted materials. Oakridge guidelines only permit copying materials specifically allowed by copyright law, fair use guidelines, license agreements, creative cornmons,[2] or proprietor's permission. Additional copyright and fair use information can be found at:

U.S. Copyright Office Fair Use

Stanford Copyright Fair Use

UMUC Copyright and Fair Use in the Classroom, on the Intemet, and the World Wide Web

Acceptable

- Use of copyrighted material with author permission
- Use of copyrighted material that meets the fair use criteria
- Use of copyrighted material that meets the common creative criteria

Unacceptable

- Using network resources to commit plagiarism.
- Unauthorized use, copying, or forwarding of copyrighted material.
- Unauthorized installation, use, storage, or distribution of copyrighted software.

[2] A tool that gives everyone from individual creators to large companies and institutions a simple, standardized way to grant copyright permissions to their creative work. The Creative Commons licenses enable people to easily change their copyright tem1s from the default of"all rights reserved" to "some rights reserved." It refers to the body of work that is available to the public for free and legal sharing, use, repurposing, and remixing.