Technology Appropriate Use Guidelines
Eugene School District 4J
May 2011

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 Eugene 4J School District's electronic communications network, 4JNet, is to be used to support and enhance learning and teaching that prepares students for success. Providing access to 4JNet is an investment in the future of both our students and staff. 4JNet supports the core beliefs of the Eugene 4J School District:

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

The Eugene School District believes that electronic communication is a tool for life-long learning, and that access to 4JNet is one of the resources that promote educational and organizational excellence. We believe the responsible use of 4JNet 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 4JNet in a responsible, efficient, ethical, and legal manner in accordance with the mission of the Eugene School District 4J. The use of 4JNet 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 4JNet. Staff members are accountable to teach and use 4JNet responsibly. Use of 4JNet 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 Internet use by minors or adults.

FERPA – 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."

Eugene SD 4J Board Policies

Board Policy KGF — Use of District Property – This policy defines 4J property including equipment, computer software, and networks, and their use by district staff and volunteers.

Board Policy JFCFA/GBNAA – Cyberbullying – "Cyberbullying" is the use of any electronic communication device to convey a message in any form (text, image, audio, or video) that violates Board Policy JB-Intimidation, Bullying, Harassment, Discrimination, Hazing, and Retaliation or which disrupts or prevents a safe and positive educational or working environment, or places a person in

reasonable fear of physical harm or damage to their property. Any form of cyberbullying, by students or staff is prohibited and will not be tolerated in the Eugene School District 4J.

Board Policy JB —Intimidation, Bullying, Harassment, Discrimination, Hazing, and Retaliation This policy defines each of the terms in the title and the consequences to students perpetrating such activity.

Definitions

4JNet	Eugene School District 4J's electronic communications network connects all school sites together with Internet access.
District 4J email	Student and staff email accounts provided by the district. (Zimbra)
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)
iPortal (Moodle)	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.wikipedia.org/wiki/Wiki - cite_note-0
Blog	Blend of the terms web and log. It is considered a type of website. 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 Eugene School District 4J 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 4JNet 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 4J Internet Guidelines Committee 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 4JNet, 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 their Technology Leadership Team (TLT) 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. District 4J'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 4JNet filter does not work outside of the district network.

Unacceptable Use of 4JNet and Equipment

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

The unacceptable uses of 4JNet 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 Policy (KGF - Use of District Property; JB - Discrimination, Harassment, Intimidation, Bullying, and Retaliation; and JFCFA/GBNAA - Cyberbullying), District Administrative Rules, or any provision in the district Student Rights and Responsibilities 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 (See Cyberbullying Board Policy)
- 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 Computing and Information Services 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 will follow the guidelines of the Collective Bargaining Agreement articles 7.2 and 7.3.

7.2 The District shall reimburse unit members for the reasonable cost of personal property with a value of $500 or less that is stolen or damaged if related to their instructional responsibilities or is stolen or damaged as a result of the District's negligence. The District shall reimburse unit members for the reasonable cost of personal property with a value greater than $500 that is stolen or damaged and is properly documented as stolen or damaged as a result of the District's negligence.

7.3 DISTRICT EQUIPMENT: Unit members will not be held liable for loss, damage or theft of District equipment provided reasonable care has been taken.

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 4JNet resources, such as email, chat, wikis, blogs, and Internet websites must be done in a responsible and respectful manner. (Student Rights and Responsibilities Handbook)

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 4J Email Accounts

All 4J staff members are issued an email account. Guest teachers, in general, are not issued email accounts. Long-term guest teachers are an exception. All 4J 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 4J committees or be asked to conduct a specific 4J 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 4J hosted web sites, wikis, blogs, and class management systems (Moodle) 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 4J 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 4J Email Accounts

General Overview

All 4J students are issued a 4J email account. All 4J Email users are expected to use commonly accepted practices.

- High school and middle school students have their 4J 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)
- Elementary students may have their district email account activated with written consent from their parents/guardian and the consent of their teacher. (Consent Form) Email accounts remain activated on a yearly basis through passive consent until the student is no longer a 4J student

---

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 4J professional teaching site, use your 4J 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. **4J 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 on-line activities. I use my Facebook account solely within the realm of my personal life

---

[1] Written by Jen Hegna, Information Systems Manager, Byron (MN) Public Schools and Doug Johnson, Director of Media and Technology, Mankato (MN) Public Schools. http://doug-johnson.squarespace.com/blue-skunk-blog/2009/8/20/networking-guidelines-revised.html

Adapted for use in the Eugene School District

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. 4J email account, 4J blog, 4J wiki…).
- Do not say or do anything using a site attached to your 4J account that you would not say or do as a teacher in the classroom. (Remember that all 4J 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 web site 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 4J 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 Eugene School District 4J, 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.

- Elementary School "Google Apps for Education" Permission Form (English)
  Elementary School "Google Apps for Education" Permission Form (Spanish)
- Middle School "Google Apps for Education" Permission Form (English)
  Middle School "Google Apps for Education" Permission Form (Spanish)

Copyright & Plagiarism

General Guidelines

Adherence to federal copyright law is required in both print and electronic environments. School Eugene District 4J 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. 4J guidelines only permit copying materials specifically allowed by copyright

law, fair use guidelines, license agreements, creative commons,[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 Internet, 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 terms 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.