Kelso School District
Acceptable Use Procedures – STAFF

Kelso School District is pleased to provide staff access to computers, electronic mail and network resources. This document contains the Acceptable Use Procedures for using these resources. Users of these resources are responsible for their actions and are expected to review and understand the procedures in this document.

Network

The district network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (blogs, websites, collaboration software, social networking sites, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network. All use of the network must support education and research and be consistent with the mission of the district. The district network has not been established as a public access service or a public forum. Users are expected to follow the rules set forth in Kelso School District Acceptable Use Procedures, Washington State K-20 Network Conditions of Use and Acceptable Use Policies (http://www.dis.wa.gov/enterprise/k20network/aup.aspx), and federal and state laws in the use of the district network. Any use of the network to access sources beyond the district network must conform to the Acceptable Use Policies of those other sources.

Network Access/ District e-Mail

1. Staff who have a signed Kelso School District Acceptable Use Agreement on file with the district will have access to the Internet.
2. Staff may request an individual or classroom e-mail account through their Building Technology Coordinator. The staff member must sign a Kelso School District Acceptable Use Agreement and have it recorded by the Human Resources department to be granted access to both types of e-mail accounts.
3. Staff will access only e-mail accounts created by the Kelso School District. Other types of e-mail accounts (e.g., Hotmail) are not permitted. *Staff members will use their district e-mail account for all job related communications.*
4. A District e-mail address is public information and will be released as appropriate under the Public Disclosure laws.
5. If users receive unsolicited e-mail messages (spam) containing inappropriate material they will delete those messages within one working day.
6. Users will not forward e-mail chain letters or engage in “spamming”. Spamming is sending an annoying or unnecessary message to a large number of people.
7. Users will check their e-mail frequently, delete unwanted messages promptly, and stay within their e-mail quota (600 messages for staff and classroom accounts).
8. Users should respect the privacy of those they correspond with before reposting a message sent to them.
9. Users should be aware that e-mail is inherently not secure. Confidentiality breaches are possible, if not likely.

Use of Personal Electronic Devices

In accordance with all district policies and procedures, staff may use personal electronic devices (e.g. laptops, mobile devices and e-readers) to further the educational and research mission of the district. Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the district network is allowed after checking with the building technology coordinator to

confirm that the device is equipped with up-to-date virus software, and is configured properly. Connection of any personal electronic device is subject to all procedures in this document. The district cannot be held liable for any damage to or theft of personal devices.

Acceptable network use by district staff includes:

1. Creation of files, digital projects, videos, web pages, social media sites, and podcasts using network resources in support of education and research; Any web pages posted on the Kelso School District network must comply with building and district standards as explained in District Web Page Authoring Procedures.
2. Accessing the Internet, participation in blogs, wikis, bulletin boards, social networking sites and groups and communicating through e-mail and webpages in support of education and research; All webpage postings or comments should be moderated by the owner and are subject to monitoring by district personnel.
3. With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately.
4. Instant messaging or video conferencing (i.e. Skype) for educational purposes.
5. Staff use of the network for incidental personal use in accordance with all district policies and procedures.

Unacceptable network use by district staff includes but is not limited to:

1. Personal gain, commercial solicitation and compensation of any kind;
2. Actions that result in liability or cost incurred by the district;
3. Downloading, installing and use of (games, audio files, video files, or other applications, including shareware or freeware) without permission or approval from the Building Tech Coordinator;
4. Downloading large files. If necessary these files can be downloaded during non-peak times such as after the school day.
5. Support for or opposition to ballot measures, candidates and any other political activity;
6. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools or any action that would degrade or disrupt system performance, individual computers, servers, or the network;
7. Unauthorized access to other district computers, networks and information systems; This includes attempting to log in through another person's account or access another person's files or resources.
8. Cyber-bullying, threats, hate mail, defamation, harassment (any kind of discriminatory jokes and remarks), and use of inappropriate or offensive language;
9. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
10. It is illegal to use the Kelso School District network to engage in any illegal act, including but not limited to, arranging for a drug sale or the purchase of alcohol, threatening the safety of persons, etc.;
11. Accessing, uploading, downloading, storage and distribution of obscene pornographic or sexually explicit material on district computers regardless whether accessing the Internet at school or home; Staff will not use the District network or District computers to access material that is profane or obscene, (that has adult oriented sexual content, such as depictions of sexual activity and nudity), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature) based on their race, national origin, gender, religion, age, disability, or sexual orientation. A person who knowingly possesses visual or printed matter depicting a minor engaged in sexually explicit conduct is guilty of a Class C felony according to Washington RCW 9.68A.070. Distributing obscene materials on the Internet is also a crime

under U.S. laws. If staff members mistakenly access inappropriate information, they should contact the Kelso School District network administrator. This will protect them against a claim that they have intentionally violated the procedures.
12. Attaching unauthorized devices to the district network; Any such device will be confiscated and additional disciplinary action may be taken.
13. It is illegal to steal or vandalize data, equipment, or intellectual property.

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by his/her own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district's computer network or the Internet.

Student Safeguards

1. Student work may be published online unless a non-disclosure form is submitted by parent or guardian. Published student work must not divulge personal information unless the website is password protected.
2. Individual, group and action photos (video or still) and audio clips in which students are not identified by name may be published on district, school, and classroom web and social media pages.
3. Pictures which identify students by name may be published on district, school, and classroom web pages and social media unless a non-disclosure form is submitted by parent or guardian.
4. Web and social media pages may not include a student's phone number, address, names of other family members, or names of friends. Teachers will monitor student postings to ensure this type of information is not disclosed.
5. Published e-mail addresses are restricted to staff members or to a general address for forwarding to a staff member. Web or social media pages may not contain any student e-mail address links or any other type of direct- response links.
6. Web or social media pages may not include any information which indicates the physical location of a student at a given time without written parental consent.
7. If students encounter dangerous or inappropriate information or messages while using the Internet, they should notify the appropriate school authority.

Filtering and Monitoring

Filtering Software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is made at the district level. Various levels of filtering may be applied to the user based on that user's individual network profile.

1. Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;
2. Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, "private" browsing sessions, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content);
3. E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;

4. The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district devices;
5. Staff members will be diligent in protecting students from viewing objectionable online content that may be inadvertently accessed when using the staff level of Internet filtering to search for educational materials.
6. Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

Use of Social Media

1. Social media is defined as any form of online publication or presence that allows end users to engage in multi-directional conversations in or around the content on the website. Social media includes but is not limited to: Facebook, Twitter, Second Life, YouTube, Google+, blogs, wikis, social bookmarking, document sharing and email.
2. Any employee creating a Professional Social Media Site must first submit a "Request to Administer a Professional Media Site" application with the building principal or department supervisor and adhere to the guidelines within that document.
3. All employees must represent themselves professionally when publishing via social media.
4. Confidential information will not be shared/posted.
5. When using social media for personal purposes, employees should be aware that what is posted online may be viewed by unintended audiences such as colleagues, parents and students.
6. Employees shall take advantage of privacy options available to them.
7. If unprofessional/inappropriate social media content is brought to the attention of administrators, disciplinary action may be enforced.

Copyright

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes is permitted when such duplication and distribution falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

Ownership of Work

All work completed by employees as part of their employment will be considered property of the district. The District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary. All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school .system. If under an agreement with the district, the work will be considered the property of the District. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

Network Security

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Staff are responsible for all

activity on their account and must not share their account password. Staff members should notify the system administrator if they identify a possible security problem.

The following procedures are designed to safeguard network user accounts:

1. Change passwords according to district policy;
2. Do not create easily guessed passwords (last name, password, admin, etc.);
3. Do not use another user's account;
4. Do not insert passwords into e-mail or other communications;
5. If writing down a user account password, it should be kept in a secure location;
6. Do not store passwords in a file without encryption;
7. Do not use the "remember password" feature of Internet browsers;
8. Lock the screen or log off if leaving the computer.

Student Data is Confidential

District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

No Expectation of Privacy/Search and Seizure

The district provides the network system, e-mail and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review and store without prior notice information about the content and usage of

1. The network;
2. User files and disk space utilization;
3. User applications and bandwidth utilization;
4. User document files, folders and electronic communications;
5. E-mail;
6. Internet access;
7. Any and all information transmitted or received in connection with network and e-mail use.

No user should have any expectation of privacy when using the district's network. Routine maintenance and monitoring of the Kelso School District network may lead to discovery of violations of these procedures or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated these procedures or the law. The investigation will be reasonable and related to the suspected violation.

The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Disciplinary Action

All users of the district's electronic resources are required to comply with the district's policy and procedures and agree to abide by the provisions set forth in the district's user agreement. Violation of any of the conditions of use explained in the district's user agreement, Electronic Resources policy or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges. In the event there is a claim that a staff member has violated these procedures in their use of the Kelso School District network, that person will be provided with a written notice of the suspected violation and an opportunity to present an explanation before a neutral administrator.