Voice Mail System

A district voice mail system is available for use at all times.

Employees assigned a voice mail extension are expected to record a greeting that includes, at a minimum, their name and an invitation to leave a message. Each school and district office is to record a greeting informing callers how to access the voice mail of the individual they seek.

Teachers are not expected to respond to calls during class time.

Use of Personal Electronic Devices

In accordance with district policies and procedures, students and employees may use personal electronic devices (e.g. laptops and mobile devices) to support and/or enhance education. Teachers and principals have final authority in deciding when and how students may use personal electronic devices in class and/or on school grounds and during the school day.

District Network

A district network has been established for the benefit of students, employees and patrons to improve communication, support education and research, and augment learning opportunities consistent with the mission of the district. The district network includes wired and wireless devices and peripheral equipment, electronic files, data storage, email and Internet content. The district reserves the right to prioritize the use of and access to the network.

Disclaimers

The district does not guarantee that the district network will be error free or that services will be uninterrupted.

The district and any businesses or agencies with which it contracts for information services will not be liable for:

- any damages to individuals or property due to information gained and/or obtained via use of the district network including without limitation, access to public networks, or
- loss of data, losses resulting from loss of data, or inability to use the network.

Filtering and Monitoring

Filtering software or services are installed and used for all computers and electronic devices with access to the Internet to block or filter access to visual depictions that are obscene, pornographic, or harmful to minors, in accordance with the Children's Internet Protection Act.

Attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited.

E-mail inconsistent with the educational and research mission of the district will be flagged as spam in district e-mail.

The district expects appropriate adult supervision of Internet use. Employees who supervise students, control electronic equipment or have occasion to observe student use of equipment online, must make a reasonable effort to monitor student use to assure that student use conforms to the mission and goals of the district. Every user must take responsibility for his/her use of the network and Internet, and avoid objectionable sites.

Internet Safety Instruction

All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response:

- age appropriate materials will be made available for use across grade levels; and
- training regarding online safety issues and materials implementation will be made available to network users.

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. Employees must obtain a student's permission prior to distributing his/her work to parties outside the school.

Login / Password Protocols

The superintendent's designees are responsible for establishing secure student and employee accounts for-all proprietary and/or confidential systems used or managed by the district.

Access to password-protected systems will be established following district receipt of the appropriate Acceptable Use Agreement signed by the user.

Logins and passwords are the first level of security for all user accounts, and are to be used only by the authorized owner of the account for authorized purposes. All users are expected to follow these procedures:

- Change passwords when required and use secure password protocols (a combination of upper/lower case letters, numbers, and/or symbols). Some systems may require a password of a minimum character length.
- Never include passwords in email communications.
- Avoid a personal list of passwords; if created, the list must be maintained in a secure location. If stored electronically, it should be password-protected or otherwise encrypted.
- Do not use the "remember password" feature of Internet browsers, especially for login to student or fiscal records systems.
- Lock your computer screen and/or log off of any accounts before leaving your computer.

The superintendent's designees will force password changes for all systems under the district's control at least annually.

Access to protected systems will be terminated upon student/staff departure from the district, unless authorized by the superintendent to continue for a specified period of time.

All use of the district network must relate to and support education or research, and must be consistent with the district's Mission Statement and this and other board policies and procedures as now written, or as may be revised from time to time. All individuals must receive appropriate training, and sign an Acceptable Use Agreement form in order to become an authorized user of the district network.

The district reserves the right to prioritize use and access to the network by students, employees, and patrons. The district reserves the right to have authorized personnel review system use as well as email file content if inappropriate activity is suspected and to remove a user's authorization to use the district network if inappropriate activity is discovered. Users should not expect that files stored on district file servers would be private. The district's wide-network provider (the k-20 Network) reserves the right to disconnect the district to prevent unauthorized activity.

Patron use may be permitted at the district's discretion. An Acceptable Use Agreement is required for each patron.

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

- Personal gain, commercial solicitation and compensation of any kind.
- Actions that result in liability or cost incurred by the district.
- Downloading, installing and use of games, audio files, video files, games or other applications (including shareware or freeware) without permission or approval from the *(insert title of position)*.
- Support for or opposition to ballot measures, candidates and any other political activity.
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools.
- Unauthorized access to other district computers, networks and information systems.
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks.
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing).
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material.
- Attaching unauthorized devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken.

The district network may be used for community-based not for profit purposes, with the advance approval of the superintendent. Such purposes include, for example: notification of events beneficial to students or the public at large, summary descriptions of services available from charitable organizations, calendars, etc.

District network users are requested to conserve system resources by deleting e-mail and unused files to free up memory provided they retain information as required by the Public Records Retention guidelines.

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, misdeliveries, or service interruptions caused by its own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting form the use of, or access to, the district's computer network or the Internet.

Student and staff work produced on or using the network is copyrighted. Parent/guardian permission is required for someone other than the student to publish the student's work.

Procedures Specific to Staff Use

Upon initial employment and/or transfer to a substantially different position in the district, all staff must sign an Acceptable Use Agreement (Form 6820-F4) indicating their understanding of district policy and procedure 6820 and their agreement to comply with acceptable use guidelines. The signed forms will be retained in the employee's personnel file.

Procedures Specific to Student Use

A student interested in obtaining an Internet account on the district's computer network, must first obtain an "Acceptable Use Packet" which includes: a letter to the student's parent/guardian (Form 6820-F1), a copy of board policy and procedure 6820, and an Acceptable Use Agreement form (Form 6820-F2). The student and parent/guardian are to review the materials in the packet. Students will be granted access to the Internet only upon receipt of the Acceptable Use Agreement signed by the student and his/her parent/guardian.

Once signed, a student's Acceptable Use Agreement will be valid for the duration of the student's enrollment in the elementary, middle or high school. When a student moves between schools, a new Acceptable Use Agreement must be signed.

The district's network administrator or designee processes and activates student accounts.

The network administrator or designee will assign an Internet account to the student within a week. Once an account has been established, the assigned supervisor will give the student a password. Students must use their own account to access the Internet. Passwords may be changed on any lab computer. To avoid potential problems, authorized students should change their password regularly and avoid use of easily guessed passwords.

Students are responsible for keeping their account and password confidential, meaning that they are not shared with any other person. All activity that occurs under a student's account and password is the responsibility of the authorized student. For this reason, students should never leave an open file or session unattended.

To use a computer in a district computer lab, each student authorized to use the Internet must:

- log into their Internet account using their account and password;
- use the provided programs to access the Internet;
- quit the session by quitting out of their Internet account and returning the computer to the initial login screen.

The network administrator or designee has the authority to check the computer logs to confirm that the student seated at a computer is the authorized student for the open account, and to periodically check to verify that the student is using their account properly. The network administrator or designee will confirm that the student has logged out, and may check cache files for inappropriate Internet access.

Names of authorized students will be listed on an Internet Eligibility List accessible to teachers. Teachers are responsible for supervision of computer use by any student in their classroom. If Internet access is necessary for a classroom project and a student does not have an Internet account or has a Denial of Consent for Individual User Access form on file, the teacher must supervise the student's use one-to-one in the classroom or must provide an alternative research project for the student.

If a student becomes aware of a security problem within the district network, among users of the district network, or on the Internet, the student must immediately notify their teacher, or a person in charge of supervising student use of computers. A student found exploiting or demonstrating a security problem is subject to the consequences identified in this procedure.

Likewise, if a student comes across information or messages that appear dangerous, inappropriate, or make them feel uncomfortable while accessing the Internet or using electronic mail or other forms of electronic communication, the student must immediately notify their teacher, or a person in charge of supervising student use of computers.

In addition to district network procedures already listed, the conduct described below is not permitted on the district network. This list is not exclusive, but serves to provide examples of prohibited conduct:

- seeking information about, obtaining copies of or modifying files, data or passwords belonging to other users;
- misrepresenting themselves or other users on the district network or the Internet;
- attempting to gain unauthorized access to the district network;
- downloading software from the Internet into the district network;
- installing software onto computers in the district network;
- making appointments without parent/guardian and/or district permission to meet people in person whom they have contacted via the district network;
- revealing their own or other's personal information (such as physical descriptions, addresses, telephone numbers) to users outside the district network. A student's own personal information may be revealed if the student has received his or her teacher's or parent's specific permission; or
- encrypting messages to avoid security review;
- sending or displaying offensive messages or pictures that disrupt the educational environment;
- using vulgar, obscene, or profane language;
- using the network to distribute harassing, threatening or intimidating communications, including hate mail or messages that violate district policies;
- accessing gambling, sexually explicit, or pornographic material through the network or using the network to store or distribute pornographic or sexually explicit materials;
- intentionally or recklessly wasting limited resources.

Consequences for Inappropriate Student Use

If a student chooses not to follow the requirements of this policy and procedure:

- access to the Internet may be revoked, and the student's Internet account will be canceled. A student without an Internet account may work on classroom Internet projects only under the one-to-one supervision of the classroom teacher in the classroom;
- additional consequences may include disciplinary action or corrective actions identified in board policy 3300. The student's principal and the superintendent will determine the appropriate additional consequences.

The duration of the loss of privileges will depend upon the severity of the student's actions, but may extend from two days to the remainder of the student's school career in the district.

Confidentiality of Student Information

With the exception of use of the Skyward secure student information system and communication within the district's Google Apps for Education access, users are to comply with district policy and the Family Educational Rights and Privacy Act (FERPA) regarding student information. The district encourages employees to use a student's namekey (first 5 letters of last name, followed by first 3 letters of first name) in all internal communications.

No Expectation of Privacy

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:

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

No student or employee should have any expectation of privacy when using the district's network. 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.