Electronic Resources: Student Acceptable Use of District Network

Scope

The following procedures apply to all District students and cover all aspects of the District network. The District network includes wired and wireless computers/devices and peripheral equipment, files and storage, e-mail and Internet content, and all computer software, applications, or resources licensed to the District. The District reserves the right to prioritize the use of, and access to, the network.

Network Access

The District expects students to exercise good judgment and use network resources in an appropriate manner. All use of the network must support education and research and be consistent with the mission of the District. Use of the electronic resources provided by the District is an expectation and privilege. In order to maintain the privilege, students agree to learn and comply with all of the provisions included in this document.

Acceptable Network Use

Includes:

A. Creation of files, projects, videos, web pages and podcasts.

B. Participation in blogs, wikis, bulletin boards, and social networking sites administered in a controlled environment, ensuring student safety and enabling the requirement to meet public record requests consistent with state and federal laws.

C. With parental permission, the online publication of student-created original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately and all copyright laws must be followed.

D. Connection of any personal electronic device is subject to all guidelines in this document.

Unacceptable/Prohibited Network Use

Includes but is not limited to:

A. Commercial Use: Using the District network for personal or private gain or benefit, commercial solicitation and compensation of any kind is prohibited.

B. Political Use: Using the District network for political purposes in violation of federal, state, or local laws is prohibited. This prohibition includes using District computers to assist or to advocate, directly or indirectly, for or against a ballot proposition and/or the election of any person to any office.

C. Illegal or Indecent Use: Using the District network for illegal, bullying, harassing, vandalizing, inappropriate or indecent purposes is prohibited.

   1. Illegal activities are any violations of federal, state, or local laws (for example, copyright infringement, publishing defamatory information, or committing fraud).
   2. Harassment includes slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, pranks, or verbal conduct relating to an individual that have the purpose or effect of creating an intimidating, hostile, or offensive environment or interfering with an individual's work or school performance, or with school operations.

3. Vandalism is any attempt to harm or destroy the operating system, application software, or data.
4. Inappropriate use includes any violation of the purpose and goal of the network.
5. Indecent activities (including accessing, storing, or viewing pornographic, indecent or otherwise inappropriate material) are in violation of generally accepted social standards for use of publicly-owned and operated equipment.

D. Disruptive Use: The District network may not be used to interfere or disrupt other users, services, or equipment. For example, disruptions include distribution of unsolicited advertising ("Spam"), propagation of computer viruses, distribution of large quantities of information that may overwhelm the system (chain letters, network games, or broadcasting messages), and any unauthorized access to or destruction of District computers or other resources accessible through the District network ("Cracking" or "Hacking").

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 its 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 network or the Internet.

Network Security and Privacy

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 purposes. Students are responsible for all activity on their account and must not share their account passwords. Password sharing is only allowed between students and their parents/guardians.

The following procedures are designed to safeguard network user accounts:

- Change passwords according to district procedure;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- If you write down your account password, keep it out of sight;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; and
- Lock (Windows button + L key) the screen, or log off, if leaving the computer.

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 a local decision.

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 or her use of the network and Internet and avoid objectionable sites.

Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are prohibited. These may include; proxies, https, special ports, modifications to browser settings or any other techniques designed to evade filtering or enable the publication of inappropriate content. This includes the use of 3G/4G networks to bypass filters.

E-mail inconsistent with the educational mission of the District will be considered SPAM and will be blocked from entering District e-mail boxes.

Staff members who supervise students, control electronic equipment or have occasion to observe student use of 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. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

Filtering will also be used to assist in the prevention of sharing personal data.

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.

Student Data

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

No Expectation of Privacy

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; information transmitted or received in connection with network and e-mail use. No student should have any expectation of privacy when using the District's network. The District reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Archive and Backup

Backup are made of all District e-mail correspondence and stored data for purposes of public disclosure and disaster recovery.

Disciplinary Action

Violation of any of the conditions of use may be cause for revoking the offender's privilege of network access and/or disciplinary action up to expulsion in accordance with district policies and

procedures. In addition, violations of this policy may result in criminal prosecutions, if warranted.

Liability

The District cannot guarantee the availability of technology resources and will not be responsible for any information that may be lost, damaged, or unavailable due to technical or other difficulties. The District cannot ensure that all electronic transmissions are secure and private and cannot guarantee the accuracy or quality of information obtained. The District will employ technology protection measures to comply with Federal and State requirements to filter or block material defined to be objectionable. However, no known process can control or censor all illegal, defamatory, or potentially offensive materials that may be available to the user on systems accessible through technology resources.

The District is not responsible for lost, stolen or damaged personal computing devices. Students bring these devices in at their own risk.

Date: 8.14