Responsible Use Procedures and Guidelines

I. Introduction

A. These procedures are written to support the Electronic Resources Policy 7396 of the Board of Directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy: successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different than face-to-face interactions.

B. It is assumed that parents grant their child the right to access the network and has a desire to have their child use network resources which includes the Internet as an educational resource unless their school has a signed Internet and Electronic Communication Exclusion form on file.

C. Use of the computer network and Internet is a privilege, not a right. A user who violates this agreement shall, at a minimum, have his or her access to the network temporarily terminated. The District may also take other disciplinary actions up to and including termination of employment or expulsion from school.

II. NETWORK ACCESS

A. The District network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content (blogs, web sites, collaboration software, social networking sites, wikis, etc.). The District reserves the right to prioritize use and access to the system.

B. Any use of the system must be in conformity to state and federal law, network provider policies and District policy.

C.. All use of the network must support education and research and be consistent with the mission of the District. From time to time, the District will make a determination on whether specific uses of the system are consistent with the regulations stated in this procedure. Under prescribed circumstances non student or staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district.

D. In accordance with all district policies and procedures, students and staff may use personal electronic devices (e.g. laptops, mobile devices and e-readers) to further the educational and research mission of the district. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day.

1. The use of personal devices on the district network is subject to available resources and may be restricted from some network resources.

2. The owner of these devices must ensure that the district and student data are adequately protected. The districts reserve the right to issue guidelines for data protection. Protection requirements may include password protection for access to the device, data encryption, and applications that can remotely remove all data from a device that has been lost or stolen.

3. All personal electronic devices (wired or wireless) including portable devices connected to the District's networks must be equipped with up-to-date virus software, compatible network card and be configured properly. Connection of any personal electronic device is subject to all guidelines in this document.

E. For security and administrative purposes the district reserves the right for authorized personnel to review system use and file content including, without limitation, the content of any email. Email is archived as per Public Disclosure Laws.

F. Acceptable network use by District students and staff includes but is not limited to:

1. Creation of files, projects, videos, web pages and podcasts using network resources in support of educational activities;

2. Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support educational activities;

3. The online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;

G. Unacceptable network use by District students and staff includes but is not limited to:

1. Using District resources for personal gain, commercial solicitation and compensation of any kind;

2. Causing any actions that result in liability or cost to be incurred by the District;

3. Downloading unlicensed or illegally obtained software applications or files;
4. Supporting or opposing political candidates, ballot measures, or any other political activity;
5.. Malicious use including but not limited to hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software, and monitoring tools;
6. Attempting to gain unauthorized access to other computers, networks and information systems;
7. Contributing to cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;

8. Posting, sending, or storing information online that could endanger others (e.g., bomb construction, drug manufacture);

9. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and

10. making use of the electronic resources in a manner that serves to disrupt the operation of the system by others, including modifying, abusing or destroying system hardware, software or other components;

H. 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.

I. 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.

III. 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 District purposes. Students and staff are responsible for all activity on their account and must not share their account password.

B. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to any entity on the system.

C. Communications may not be encrypted so as to avoid security review.

D. These procedures are designed to safeguard network user accounts:

1. Avoid easily guessed passwords;
2. Change passwords according to District policy;
3. Do not use another user's account;
4. Do not insert passwords into e-mail or other communications;
5. If you write down your account password, keep it secure;
6. Do not store passwords in a file without encryption;
7. Do not use the "remember password" feature of Internet browsers; and
8. Lock the screen, or log off, if leaving the computer.

E. The District reserves the right to remove a user account on the system to prevent unauthorized activity. The District's wide area network provider reserves the right to disconnect the District to prevent unauthorized activity.

IV. INTERNET AND ELECTRONIC COMMUNICATION

Access to the Internet is an important educational tool that enables students to, learn, share, collaborate, communicate, and develop the skills necessary to succeed in a digital world. The district will provide access to educational online resources to further the education of our students. These resources may include relevant educational websites through subscription databases and other services that allow students to research, create and share work.

Students will have access to the Internet unless their school has a signed Internet and *Electronic Communication Exclusion* form on file.

A. Electronic Mail for staff and students

1. The school district will provide access to electronic mail for all staff members.

2. The use of email must comply with all other requirements in this document.

B. Internet Safety: Personal Information and Inappropriate Content

1. Students should never reveal personal information, such as complete names, addresses and telephone numbers and identifiable photos web sites, blogs, podcasts, videos, social networking sites, wikis, e-mail or as content on any other electronic medium without permission from their teacher, a parent, or guardian. No staff member may disclose use, or disseminate personal identification information

regarding minors other than for legitimate educational purposes without authorization.

2. Students are prohibited from making appointments, without parental permission, to meet people in person who they have contacted through the Internet, email, or other forms of electronic communication.

3. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission.

4. Using student pictures and work promotes learning, collaboration and provides an opportunity to share achievements. It is assumed that parents grant the right for the District to post a students' picture or work on the web unless their school has a signed *Directory of Information Opt Out* form on file.

5. Prior to the posting of student pictures or work on any public class, school, or district website, the appropriate permission will verified according to District policy.

6. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

D. CIPA UPDATE/Internet Safety Instruction

1. 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.

2. Age appropriate materials will be made available for use across grade levels.

3. Training on online safety issues and materials implementation will be made available for administration, staff and families.

V. Filtering and Monitoring

A. 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.

B. Filtering software is not 100% 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 or her use of the network and Internet and avoid objectionable sites;

C. Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to District browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;

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

G. 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 computers;

H. 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

I. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

VI. Copyright

All users of the Network shall comply with current copyright laws.

A. 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 are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

B. While all student work is copyrighted it is assumed that parents grant the right for the District to post student work on the web for educational purposes unless there is a signed *Directory of Information Opt Out* form on file with the school.

VII. Student Data is Confidential

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

VIII. No Expectation of Privacy

A. 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; and
7. Any and all information transmitted or received in connection with network and e-mail use.

B. No student or staff user 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.

IX. Archive and Backup

A. Backup is made of all District e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are

backed up on District servers regularly. Refer to the District retention policy for specific records retention requirements.

X. Disciplinary Action

All users of the District's electronic resources are required to comply with the District's policy and procedures. Violation of any of the conditions of use explained in the Electronic Resources Policy or in these procedures could be cause for disciplinary action ranging from revocation of network and computer access privileges up to and including expulsion from school or termination of employment. In addition, violations of this policy may result in criminal prosecutions, if warranted.

MMS Disciplinary Action Plan for Electronic Device Violations

Expectation – Electronic devices are not out (visible) during instructional time without permission from the teacher. Electronic devices cannot be used to photograph, record or videotape others without their permission.

1st Violation – The Classroom teacher will confiscate and return at end of class. NOT recorded in SkyWard, teacher keeps track.

2nd Violation – Teacher will confiscate and deliver to office. Violation recorded in SkyWard, electronic device returned to student at the end of the day.

3rd + Violation – Teacher will confiscate and deliver to office. Violation recorded in SkyWard, parent contacted, electronic device returned to parent OR student after 24 hours.

Picture/Video/Voice Record Violation – will be treated as a 3rd offense. Violation recorded in SkyWard, parent contacted, electronic device returned to parent OR student after 24 hours.

In addition –

-Any electronic devices out/visible in locker rooms or restroom will be confiscated and returned to ONLY to parent. Electronic device use in locker room and bathroom areas may result in additional consequences for harassment or bullying.

-Non-compliance or arguing with staff over confiscation will be disciplined as appropriate as an additional offense. Students are expected to surrender their electronic devices to staff upon request.