MEAD
SCHOOL DISTRICT

Procedure 2022
INSTRUCTION

ELECTRONIC RESOURCES

K-20 Network Acceptable Use Guidelines/Internet Safety Requirements

These procedures are written to support Policy 2022, Electronic Resources, and to promote positive, ethical 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 a person's life and career. Individuals safeguard their personal safety online and protect the confidentiality of staff and student data and the integrity of district programs to which they have access.

Network Etiquette

Responsible personal conduct within the online environment is no different from responsible personal conduct face-to-face. Generally accepted rules of network etiquette include, but are not limited to the following:

A. Be polite and ethical.
B. Do not be abusive or harassing in your messages to others.
C. Do not swear or use vulgarities or any other language inappropriate in a school setting.

Use of Interfering and Communication Devices

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. District staff will retain the right to determine which devices may be activated, while 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.

Except as set forth below, a student may possess, but may not operate or engage, any interfering device (i.e. cell phone, smart phone, camera) during school hours unless specifically authorized in advance by the school personnel in charge of the class or activity.

A. During any time when a student is scheduled to be in class or involved in a regular school activity, it is a violation of policy for the student to have in the student's possession an electronic communication device or camera which is in the "on" position and ready to receive, send, capture, or record any communication, visual image, sound, text message or other information.

B. Electronic communication devices and cameras must not be activated or utilized at any time by any person, to include a student, teacher, staff employee, patron, or any other individual, in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include but are not limited to locker rooms, shower rooms, restrooms, and any other areas where students or others may change or be in any stage or degree of disrobing or changing clothes.

C. At no time may any electronic communication device or camera be utilized by any student in any way to threaten, humiliate, harass, embarrass, bully or intimidate others.

D. Electronic communication devices and cameras must not be used to cheat on tests/exams or to engage in passing or transmitting otherwise secure information, i.e., electronic forgery.

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. No one may access the network without having signed and returned a Network Contract.

Acceptable network use by district students and staff includes:

A. Creation of files, digital projects, videos, web pages and podcasts using network resources in support of education and research.

B. Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and webpages that support education and research.

C. 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.

D. Staff use of the network for incidental personal use in accordance with all district policies and procedures.

E. Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the district network after checking with the director of technology or designee to confirm that the device is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all procedures in this document.

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

A. Actions for personal gain, commercial solicitation and compensation of any kind.

B. Online purchase of any product or service by students, who will be held financially responsible, along with their parents, for any fees or costs that result from said purchase.

C. Actions that result in liability or cost incurred by the district.

D. Downloading, installing and/or using games, audio files, video files or applications (including shareware or freeware) by students without permission or approval from the instructor.

E. Excessive network use, i.e., mass emails, chain letters, “spamming” or denial of use actions or excessive storage of personal files, i.e., music, video, photos or data.

F. Support for or opposition to ballot measures, candidates and any other political activity.

G. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools.

H. Using an account other than your own or making any attempt to gain unauthorized access to accounts on the network.

I. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks.

J. Posting, sending or storing information online that could endanger others (e.g., bomb construction, drug manufacture) or that violates federal state or local law.

K. Accessing, viewing, uploading, downloading, storing and/or distributing obscene, pornographic or sexually explicit material.

L. Attaching unauthorized devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken.

Hold Harmless

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data, personal or district-related, resulting from delays, non- deliveries, mis-deliveries or service interruptions caused by his/her own negligence or by equipment or network failure for any cause 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. The District makes no guarantee of the accuracy or completeness of information obtained over the network.

Internet Safety

Personal Information and Inappropriate Content:

A. Students and staff should not reveal personal information, including a home address and phone number or school name on web sites, blogs, podcasts, videos, social networking sites, wikis, e-mail or as content on any other electronic medium without appropriate authorization.

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

C. No student pictures or names may be published on any public class, school or district website unless the appropriate permission has been obtained according to district policy.

D. Parents / Guardians should be aware the district provides an email account for each student above 4th grade.

E. Students who encounter dangerous or inappropriate information or messages should notify the appropriate school authority.

F. Be aware that long-lasting implications may attach to texting, posting images or publishing information in the online environment.

G. Students should never make plans to meet in person someone encountered online without parent or guardian permission.

CIPA UPDATE/Internet Safety Instruction

Students and staff will be provided with materials instructing them about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

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

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

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 may also be filtered. The determination of what constitutes "other objectionable" material is a local decision.

A. 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. Individuals retain responsibility for choices regarding internet sites and use.

B. Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content).

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

D. 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.

E. 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.

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

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. Plagiarism, that is, copying or reproducing the ideas, images or text of others without assigning appropriate credit, is prohibited.

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.

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. Students and staff are responsible for all activity on their accounts.

The following procedures are designed to safeguard network user accounts:

A. Do not share passwords to your accounts with anyone.
B. Staff should change passwords to accounts that permit such changes at least yearly, using proscribed formats and avoiding district, school or mascot names or other easily guessed passwords.
C. Individuals who believe their passwords have been compromised must contact technology services as soon as possible.
D. Do not use another user's account.
E. Do not insert passwords into e-mail or other communications.
F. If you write down your user account password, keep it in a secure location.
G. Do not store passwords in a file without encryption.
H. Do not use the "remember password" feature of Internet browsers or online programs or use the "stay signed in" feature available in some programs and applications.
I. Lock the screen or log off if leaving the computer.

Student Data is Confidential

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

No Expectation of Privacy

Our district provides the network system, e-mail and Internet access as tools 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:

A. The network.
B. User files and disk space utilization.
C. User applications and bandwidth utilization.
D. User document files, folders and electronic communications.
E. E-mail.
F. Internet access.
G. Any and all information transmitted or received in connection with network and e-mail use.
H. Or any other electronic resources not specifically named above.

No student or staff user should have any expectation of privacy when using the district's network. Computers on the network may be subject to real-time remote viewing without prior notification. Communications may not be encrypted so as to avoid security review. The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents and files, personal or otherwise, if stored in our electronic resources, are subject to the public records disclosure laws of the State of Washington.

Archive and Backup

Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Refer to the district retention policy for specific records retention requirements.

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 Network Use Contract). Violation of any of the conditions of use explained in the Network Acceptable Use Contract, Electronic Resources policy or in these procedures by staff members will result in progressive discipline up to and including discharge. Violations by students could be cause for disciplinary action and/or legal action, including, but not limited to, suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Adopted: May 13, 1997
Revised: June 10, 2002
Revised & Renumbered: May 7, 2012