Staff Responsible Use Procedure

K-20 Network Responsible Use Guidelines/Internet Safety Requirements

In support of Policy 5254, Electronic Information Systems, and to provide staff with Responsible and appropriate usage guidelines, these procedures support and promote positive and effective digital citizenship among Staff. Digital citizenship represents more than technology literacy. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. These procedures are intended to support the education of students and operation of district business. Violation of these procedures may be cause for disciplinary action, up to and including termination of employment.

Network Use

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 within its discretion to prioritize the use of, and access to, the network and deny access to particular websites. All use of the network must support education and research and be consistent with the mission of the district.

The following rules and procedures constitute the Responsible Use Procedure for use of the district's electronic information systems. Each user of the system must abide by these rules in order to access and use the system. Responsible Use Procedure includes, but are not limited to:

Responsible network use by district 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 web pages that support educational research;
C. Publication of original educational material, curriculum related materials and student work with appropriate permissions. Sources outside the classroom or school must be cited appropriately; and
D. Incidental personal use in accordance with all district policies and guidelines.

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

A. Personal gain, commercial solicitation and compensation of any kind;
B. Actions that result in liability or cost incurred by the district;
C. Support for or opposition to ballot measures, candidates and any other political activity;
D. Information posted, sent or stored online that does not support the district mission;
E. Disruption or damage of systems or changes to hardware, software, or monitoring tools;
F. Unauthorized access to other district computers, networks and information systems;
G. Accessing, uploading, downloading, storage and distribution of criminal, illegal, obscene, pornographic or sexually explicit material;
H. Attaching unauthorized equipment to district network services. Any such equipment will be confiscated;
I. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks, posts, files or comments on social media sites. The district reserves the right to remove any user-generated content from its sites at any time; and,
J. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs.

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, miss-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.

Internet Safety: Personal Information and Inappropriate Content

A. Staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, social networking sites, wikis, and e-mail or as content on any other electronic medium.
B. Staff should not reveal personal information about another individual on any electronic medium without first obtaining permission.
C. No student pictures or names can be published on any public teacher, club, school or district website unless the appropriate permission has been obtained according to district policy.
D. If a staff member encounters dangerous or inappropriate information or messages, they should notify the appropriate district 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 a local decision.

A. 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;
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; and
D. Staff must maintain an appropriate level of familiarity with the Internet to monitor, instruct and assist effectively and maintain student safety.

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 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. All users utilizing YCS network shall comply with current copyright laws and Policy 2028, Copyright Compliance.

All student work is copyrighted. Permission to publish any student work requires permission from the student and parent/guardian.

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. Staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard network user accounts:

A. Change passwords according to district policy;
B. Do not use another user's account;
C. Do not insert passwords into e-mail or other communications;
D. Storing passwords in a file with encryption;
E. Do not use the "remember password" feature of Internet browsers; and
F. 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).

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 and parent/guardian's permission prior to distributing his/her work to parties outside the school.

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:

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

No staff 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.

Archive and Backup

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 files are backed up on district servers regularly. Refer to the state 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 district's Responsible Use Agreement. Any user who violates district Responsible Use Procedure may be denied access by the district or if deemed severe enough, discipline sanctions, including suspension, may be imposed over and above access privilege revocation. In certain instances the district may be required to notify local and/or federal law enforcement agencies of potential criminal behavior.

Accessibility of Electronic Resources

Federal law prohibits people, on the basis of disability (such as seeing and hearing impairments), from being excluded from participation in, being denied the benefits of, or otherwise being subjected to discrimination by the district. To ensure that individuals with disabilities have equal access to district programs, activities, and services, the content and functionality of websites associated with the district should be accessible. Such websites may include, but are not limited to, the district’s homepage, teacher websites, district-operated social media pages, and online instructional materials.

District staff with authority to create or modify website content or functionality associated with the district will take reasonable measures to ensure that such content or functionality is accessible to individuals with disabilities. Any such staff member with questions about how to comply with this requirement should consult with the designee of the Superintendent.

I understand my responsibility in using technology for district related business.

Print Name

Date

Signature