INSTRUCTION

Technology and Electronic Resources

These procedures are written to support implementation of Policy 2180, Technology and Electronic resources, and to promote positive and effective digital citizenship among students and staff that is consistent with District policy and the mission, goals, and purpose of the District. Staff and students should 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 from in-person interactions.

1. Network

The District network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (blogs, websites, collaboration software, 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, goals, and purpose of the District.
Acceptable network use by District students and staff includes the following used in accordance with District policies and guidelines:

A. Creation of files, digital projects, videos, web pages, podcasts, etc. using network resources in support of educational purposes;
B. Participation in blogs, wikis, bulletin boards, pre-approved social networking sites and groups, and the creation of content for podcasts, e-mail and webpages that support educational purposes;
C. With parent/guardian permission, the online publication of original educational materials, 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.

Unacceptable network use by District students and staff includes, but is not limited to the following:

A. Personal gain, commercial solicitation and compensation of any kind;
B. Liability or cost incurred by the District;
C. Downloading, installing and use of games, audio files, video files, games or other applications (including shareware or freeware) for purposes other than education without permission or approval from the Technology Department. Any such files may be removed by the District without notice;
D. Support for or opposition to ballot measures, candidates, and any other political activity;
E. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs, and changes to hardware, software and monitoring tools;
F. Unauthorized access to other District computers, networks and information systems;

G. Cyberbullying, hate mail, defamation, harassment and/or retaliation and/or discrimination of any kind;
H. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
I. Accessing, uploading, downloading, storage and/or distribution of obscene, pornographic or sexually explicit material;
J. Causing or attempting to cause security breaches or disruptions of network communication and/or network performance; or
K. Connection to the network of personally owned computers, electronic devices, or other equipment without prior approval from the superintendent or designee. Any such equipment may be remotely disabled, confiscated, and/or removed. This does not apply to authorized WiFi access.

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 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.

2. Internet Safety and Instruction

Personal Information and Inappropriate Content:

A. Students and staff will not reveal personal information, including a home address and phone number on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium;
B. Students and staff will not reveal personal information about another individual on any electronic medium;
C. Staff will not interact with students in a personal manner on Internet social networking sites such as Facebook, MySpace, Twitter, or any similar sites;
D. No student pictures or names can be published on any public class, school or District website unless the appropriate permission has been verified according to District policy;
E. Offensive, objectionable, inappropriate content, or content inconsistent with District policies that is posted on District-owned or operated Internet sites or pages will be deleted at the discretion of the superintendent or designee.

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

3. Filtering and Monitoring

Filtering software is used to block or filter access to materials 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 determined by the superintendent or designee.

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 lone solution. Every user must take responsibility for his/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. This includes, but is not limited to 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; and
F. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

4. Supervision and Access

Staff and students who access the Pasco School District Network should receive appropriate training and/or information regarding acceptable use. A signed "Internet Use Informed Consent" form, or other similar form adopted by the District, must be on file with the District for students to have independent access to the internet consistent with District acceptable use. Staff must sign a "Network Account Application" assurance form, or other similar form adopted by the District.

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 use of this equipment to ensure that student use conforms with this policy and procedure.

Under prescribed circumstances, guest, vendor, or contractor use of the network may be permitted, provided such individuals agree that their use furthers the purpose and goals of the District, and is consistent with this policy and procedure.

5. 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.

6. 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 permission prior to distributing his/her work to parties outside the school.

7. Network Security and Privacy

1. 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 account and must not share their account password. The following procedures are designed to safeguard network user accounts:

A. Change passwords according to District requirements;
B. Use of another user's account is strictly prohibited;
C. Do not insert passwords into e-mail or other communications;
D. Memorize account passwords and/or keep them in a secure location;
E. Do not store passwords in any electronic file without encryption;
F. Do not use the "remember password" feature of Internet browsers; and
G. Lock the screen or log off if leaving the computer.

2. Student Data is Confidential

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

3. 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, restrict access to, 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 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 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.

8. 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 and student files are backed up on District servers regularly. Refer to the District retention policy for specific records retention requirements.

9. 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 network account application, any user agreement, or this policy and procedure may be cause for disciplinary action, up to and including suspension or expulsion from school (for students), up to and including suspension or termination of employment (for staff), and suspension or revocation of network and computer access privileges.

10. Social Networking Sites/Interactive Media

1. General Conditions

The District's electronic resources may include District established social media sites or accounts, such as Facebook pages, Twitter, or other similar interactive media that are created and maintained by the superintendent or designee. Policy 2180 and 2180P apply to members of the public accessing and/or posting to such sites, and any violation of these requirements shall result in removal of prohibited content and/or denial of access privileges for violators. Members of the public may post relevant content on such District-maintained sites if account permissions are set to allow such posting, provided that any such content complies with the requirements of Policy 2180 and 2180P.

Written authorization is required from the superintendent or designee to create or establish social media sites, web pages, or other interactive media sites related to the District, any District school, classroom, department, or activity. Creation of such sites without permission is strictly prohibited.

2. Removal of Posted Material

The District's electronic resources that allow members of the public to post comments on District-established web sites are not intended to create a public forum for the exercise of first amendment rights. Instead, they are intended to facilitate and support the District's educational mission. The District will remove posted materials that fail to comply with Policy 2180 and 2180P, and/or he following guidelines:

A. All content must be directly and materially relevant to the District-sponsored content that invites public comment or responses.
B. Content may only use language, style and tone that is generally acceptable for publications intended to reach school-aged children and families, and that is consistent with the District's educational mission generally and its goals of teaching civility, respect, and reasoned dialogue. Content that is false, harassing, threatening, abusive, vulgar, indecent, obscene, defamatory, libelous, or harmful to minors in any way; content that involves misrepresentations or personal attacks; and content that demeans or disparages an individual or group of individuals, is prohibited.
C. Persons may not make allegations or disclose personal information regarding students.
D. Content may not include advertising, promotion of commercial services or products, solicitation of funds for any purpose, or statements in support or opposition of political candidates or ballot propositions. Posting links to web sites or other electronic content, unless inherent in the social network involved, is prohibited.

The District does not express approval or support for the views expressed by third parties. The District may, in its discretion, respond to posted materials when doing so may facilitate or support the District's educational mission. Any response or lack of response should not be interpreted as an expression of approval or support. Individuals who desire a response to a complaint regarding the District's personnel or programs should follow the complaint process in Board Policy 4312. In addition any request for public records may not be submitted on social network or interactive media sites and instead must be submitted in accordance with Board Policy 4340.

3. Removal of Posted Materials, Denial of Access and Review Procedure

The District may remove posted content for violation of this policy and procedure, or other District policies or law at any time. The District may also deny repeat violators posting and/or viewing privileges. A person who desires to appeal a District action removing a posting or denying access privileges may file a complaint with the District pursuant to Board Policy 4340.