Port Angeles School District Administrative Procedure Electronic Resources and Internet Safety

Electronic Resources

The district provides the electronic communications system for its students and staff members. The components of the electronic communications system include, but are not limited to, the computer network, both local and wide area, servers on those networks, the computer workstations, the email system, access to the internet, and cell phones connected to our network.

District computers are intended for school use, not for personal use. School computers belong to the school, not the person using them.

Student Internet Access

It is assumed that students will be accessing the electronic communications system including, but not limited to, the internet, Google Apps for Education, and Microsoft Office 365 on a routine basis. **Parent/Guardian must sign an Internet Opt-Out form** (2022F) in order to inform the district if they do **not** wish their student to have access to the internet, Google Apps for Education, and Microsoft Office 365.

Access to electronic communications systems

Computer resources are to be used exclusively to support the instructional and business objectives and policies of the district. All staff members must sign and adhere to the Internet User Agreement.

- All existing district rules apply to staff members' conduct when using electronic communication systems, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of district resources, sexual harassment, information, data security, and confidentiality.

- Staff members are expected to communicate in a professional manner consistent with state laws governing the behavior of staff members and with federal laws governing copyright. Communications over the network are often public in nature; therefore, general rules and standards for professional behavior and communications will apply.

- While direct connection to electronic communication systems offers a cornucopia of potential benefits, it can also open the door to some significant risks to data and systems if staff members do not follow appropriate security discipline. A staff member may be held accountable for any breaches of security or confidentiality resulting from misuse of the district's electronic communication systems.

- Reports of inappropriate behavior, violations or complaints will be routed to the staff member's supervisor for appropriate action. Violations may result in disciplinary action

consistent with district policies and regulations regarding staff members' conduct, up to and including termination.

Unacceptable use is defined to include, but is not limited to, the following:

- Copying and/or downloading any commercial software or other material in violation of federal copyright laws.
- Use of the network for financial gain, or illegal activity.
- Use of the network to download, store, and copy or transmit pornographic, racist, sexist or other offensive or derogatory material.
- Any form of vandalism, including but not limited to, damaging computers, computer systems or networks, other user files, and/or disrupting the operation of the network.
- Use of profanity, obscenity or other language that may be offensive to another individual.
- Accessing another individual's account or a restricted account without prior consent. (Passwords should be frequently changed and never shared.)
- Management of personal finances.
- Conducting any form of personal transaction, personal business, Ebay, etc.
- Any other conduct which may constitute a violation of district policy.

Back-up Information

The district is not responsible for loss of information from misuse, malfunction of computing hardware and software, or external contamination of data or programs. The district will make every effort to ensure the integrity of its computer systems and the information stored thereon. However, staff members and students must be aware that no security or back-up system is 100% reliable.

Each computer user is responsible for making and keeping a back-up of their data. Routine back-ups or saving are a normal expected part of computer use as a part of each staff member position. If staff members need help creating a back-up of their data, they can contact the technology department or refer to the technology web page for instructions.

Care, responsibility and use of district owned equipment.

District property is self-insured through district funds, however, if the property, i.e. district laptop is taken off site then the responsibility for the cost to replace any equipment that is stolen, lost, or damaged is to the staff members.

Copyright

It is the intent of the district to adhere to the provision of copyright laws in all areas including the internet. Illegal copies of copyrighted material may not be made or used on district equipment.

Copyright Violation Guidelines

- Under current US law, all creative efforts are copyrighted the moment they are first put on paper, input into a computer, or recorded in any tangible form. While registration or stating that an item is copyrighted could increase the penalties to an infringer and the monetary return to the copyright holder in a civil suit, copyright notice is not required.
- Copyright is violated whether a fee is charged or not.

- Postings to the internet are not automatically in the public domain and do not grant permission to do further copying.
- Copyright is not lost simply because it is not defended.
- Copyright exists in civil law and criminal law. Criminal fines start at $10,000 per violation.
- Every attempt should be made to get permission from the copyright holder prior to republishing any material.

Copyright Violation and Software Piracy

- The district forbids the use, distribution, or installation of any software not owned by the district or school.
- All school owned software must have a copy of the license kept in a secure file in the school and another copy sent to the Director of Educational Technology.
- The district reserves the right at any time, without notification, to uninstall, remove or delete any software, from any computer or network server, which does not comply with district software policy.

Disclaimer of Liability

The district will not be liable for the staff members' or students' inappropriate use of the district's electronic communication resources or violations of copyright restrictions, staff members' or students' mistakes or negligence, or costs incurred by staff members' or students'. The district will not be responsible for ensuring the accuracy or usability of any information found on the internet.

The district shall not be responsible for any damages to the user from the use of the computer system, including loss of data, non-delivery or missed delivery of information or service interruptions.

E-mail

E-mail creates a permanent record that may be archived and retrievable at a later date, even though the user has deleted it. E-mail is subject to the district document retention policy. Be cautious about what you send and to whom. E-mail is a public record which may be examined by any individual at any time. There is no expectation of personal privacy in such communications.

- E-mail attachments may introduce viruses. Be cautious of the origin of an email; if the e-mail includes an attachment, do NOT open it – delete it immediately.
- E-mail items older than 90 days may be purged from the servers.
- Staff members may not use their district-provided email account for personal, non-school related communications, monetary gain, political/religious advocacy, union activities not approved by negotiated agreement, or private business enterprises.

Large file downloads and network bandwidth

Internet radio and music and video downloads that are not directly related to instruction or expressly authorized can overload the network bandwidth and are prohibited. Computers purchased by the district are provided solely as a resource for instructional or job-specific uses. Limit use of bandwidth intensive resources during peak hours (7:30 AM to 3:00 PM) so that available bandwidth can be reserved for student instructional use.

Limitation/termination/revocation of system user's access
The district may limit, suspend or revoke a system user's access to the district's system(s) upon violation of district policy and/or procedures.

Privately owned devices
Anyone who brings their privately owned device on district property or while attending district sponsored or district related activities is personally responsible for the equipment. Responsibility for the maintenance and repair of the equipment rests solely with that individual, including installation of software and configuration of peripherals. Any damage to the equipment, including results from viruses, is the responsibility of the individual.
Software residing on privately owned devices must be personally owned unless authorized by the district and within the licensing constraints of the software company. The district retains the right to determine where and when privately owned equipment may be attached to the network.

Software Downloads
The only software that may be installed on a district computer is software that has been approved by the Director of Educational Technology or designees. No executable files of any sort may be downloaded from the web onto district computers. This specifically includes (but is not restricted to) screen savers, utility programs, instant messenger services, games or music. No software is to be brought from outside the district to be installed on district computers without the approval of the Director of Educational Technology or designees.

Director of Educational Technology Responsibilities
The Director of Educational Technology as well as the building Principal or designee at the school will do the following:

- Disseminate and enforce district policy, administrative rules and regulations for the network and guidelines for students and staff member access.
- Ensure that all staff members supervising students who use the district's system(s) provide training emphasizing the appropriate and responsible uses.
- Monitor or examine all system(s) activities deemed appropriate to ensure proper use of the system(s).
- Set limits for computer storage utilization on the system(s) as needed.

Vandalism
Any malicious attempt to harm or destroy district equipment, materials, or user data, is prohibited. Deliberate attempts to compromise, degrade or disrupt system performance or operation will be viewed as violations of district policies and procedures and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the placement, transmission or creation of computer viruses or other data or programs that negatively impact the computer or system.

Internet Safety

Filtering software

To the extent practical, technology protection measures (internet filter) shall be used to block or filter the internet, and other forms of electronic communications to prevent access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or pornographic, or to any material deemed harmful. Technology protection measures may be disabled or minimized for bona fide research or other lawful purposes.

In order to address the issue of inappropriate Web-based material and to comply with the Child Internet Protection Act, the district has installed an internet filtering system.

- All Web-based content accessed through computers connected to the district network is filtered through this system.
- Installation and operation of this or any internet filtering system on district computers does not preclude staff members, students and community members from their responsibility to use the network services responsibly.
- In some cases, sites with educational value that are inadvertently blocked may be considered for review. Only district personnel may submit a request to unblock a site. The staff member may submit a detailed request to their building administrator describing intended use in the curriculum or other job related function.
- In other cases, objectionable sites may not be identified by the filter and may need to be blocked. Anyone with a concern about an objectionable site may submit a request for review to the building principal or designee or Director of Educational Technology.
- While every effort will be made to act on blocking and unblocking requests as quickly as possible, in some cases the review may take 3-5 days. Those submitting a request will be notified when a decision is made. The individual must provide the exact URL code (copy and paste into the email) in order for the site to be reviewed.

It shall be the responsibility of all staff members to supervise and monitor usage of the online computer network and access to the internet in accordance with this policy and the Children's Internet Protection Act.

Privacy

There can be no expectation of privacy on any device in the district, including privately owned devices that are used over district internet access or are related to fulfillment of district staff member responsibilities. Staff members must be aware that all information accessed, created, sent, received or stored on a district computer and the network is not private.

- While the district respects the privacy of staff members or students and does not have a practice of monitoring or reviewing electronic information, the district reserves the right to do so for any reason.
- The district may monitor and review activity in order to analyze the use of systems, monitor compliance with policies, conduct audits, or obtain information for other reasons.
- The district reserves the right to disclose any electronic message to law enforcement officials, the public or other third parties.

- Instructional or school-related records stored on personal privately owned electronic devices may be subject to disclosure as public school records so their use for school or student communication purposes is cautioned.

Publishing Student Information on the Web

- No home phone numbers or addresses of students may be published.
- Students shall not include personal information that would permit others to determine the location of the student at any given time. This includes place of employment, specific times and dates of extracurricular activities, class schedules, and other information that poses a safety concern for the student.
- Content on the Web pages(s) must comply with the internet user agreement.
- Links to student web pages not located on the district web servers may not be made from the schools' or districts' web pages.

Social Networking Sites

While a staff member may use social networking sites in his/her personal life, it is not appropriate to "accept" students as "friends' who may wander onto his/her page or seek to elicit such a contact. Nor is it appropriate to seek out or search for students for the purposes of establishing a personal social media connection. If a staff member has already accepted students onto his/her personal social networking page, set a boundary for them to follow such as:

- All staff members have been asked by the district to use district communication mechanisms to communicate with students. If you wish to contact me, my school email address is: _____ and my school voice mail is _____. I look forward to working with you at school.

Any use of social media for school-related purposes or instruction must fulfill an educational purpose.

Revised: 11/30/2023