HUMAN RESOURCES

Technology

The use of district technology by Port Townsend Public Schools employees is vital to its daily activities. Effective instruction and efficient operation and management require a staff that is skilled in the use of technological tools. Ongoing training is essential.

Additionally, Port Townsend Public Schools permits the use of mobile electronic communication devices ("ECDs", e.g., smartphones, tablets, slates, notebooks, laptops, cellular phones, and other similar mobile electronic communication devices). We believe that an ECD can play a positive role in furthering our staff and students' learning. The Port Townsend Public Schools wireless network permits individuals with a district network account and an ECD to access the internet.

Access

Employees will have access to job-appropriate technologies and software applications while being provided opportunities to use those technologies and software applications.

Appropriate Use

1. It is the expectation of the district that employees effectively and appropriately use available technology. Employees will adhere to the Technology Acceptable Use Policy.

2. Inappropriate use should be reported to appropriate district officials.

3. All users of district technology will comply with current copyright laws.

General Use of Port Townsend Public Schools Technology

1. Diligent effort by all users must be made to conserve system resources; e.g., system storage, network bandwidth, software licenses, etc.

2. Prior to employees having access to district technology, every effort will be made to provide appropriate training.

Personal Security and Internet Safety

Staff should not share personal information about employees with students without appropriate authorization.

Personal Information and Inappropriate Content:
- Students and staff should 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.

- Students and staff should not reveal personal information about another individual on any electronic medium.

- No student pictures or names can be published on any class, school or district web site unless the appropriate permission has been verified according to district policy.

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

District Network Use

1. All use of district technology equipment and network is intended to be in support of education and Port Townsend Public Schools' operations and should be consistent with the mission of the district. Port Townsend Public Schools reserves the right to prioritize use and access to the district technology equipment and network. Some personal use is permitted as long as such use does not violate PTSD's policies and does not interfere with school-related performance of job duties.

2. Any use of district technology equipment and network must be in conformity with state and federal law, and network district policies and procedures.

3. Use of district technology equipment and network for commercial solicitation is prohibited except as allowed by law.

4. Use of email or other technology is intended for school-related communication and should avoid the promotion of personal interests and/or the solicitation of support for purchasing items such as, but not limited to: yard sales, Tupperware parties, Pampered Chef parties, Girl Scout Cookies, holiday wreaths for service groups, etc.

5. District technology constitutes public facilities and may not be used to support or oppose political candidates or ballot measures

6. When using school district technology, subscriptions to mailing lists, bulletin boards, chat groups, commercial online services or other information services must be directly related to classroom curriculum or the job responsibilities of the employee.

7. District technology and/or personal ECDs will not be used to disrupt the operation and use of district technology by others. District technology, including hardware and software, will not be destroyed, modified, removed or abused in any way.

8. Use of district technology to develop programs or institute practices that harass other users or gain unauthorized access to any technology service or information and/or damage to the components of a technology service or information are prohibited.

9. Users are responsible for the appropriateness of the material they transmit or publish. Use of district technology to access, store or distribute obscene, pornographic, or sexually explicit material is prohibited.

10. The use of district technology, including district cell phones, to conduct and communicate district business via email, district social media and text are all subject to the Washington Public Records Act. Thus, text messaging on district cell phones is discouraged except for emergencies, safety-related matters or to communicate routine, non-substantive time-sensitive matters. Email is preferred.

11. Physically connecting or attaching any computer, networking equipment or device to district technology via network ports and/or communications closets, by anyone other than a network technician or other individuals expressly authorized by the director of Educational Technology Services is prohibited. Unauthorized computer or networking equipment or components will be removed without notice and immediately investigated for security violations.

Use of Personal Electronic Communication Devices and Accounts

Staff may possess and use personal wireless/Wi-Fi ECDs, provided that such devices do not pose a threat to academic integrity, disrupt the learning or work environment or violate the privacy rights of others. There should be no expectation of privacy when using the district's network. District business should not be conducted on personal devices. However, if an employee does conduct district business on their personal ECD or using personal email or personal social media accounts, a public record is created regardless of who owns the ECD and whether the account is personal.

The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate.

Staff in possession of personal ECDs will observe the following conditions:

1. The Port Townsend Public Schools wireless network will provide filtered Internet access. Port Townsend Public Schools is not liable for access to any other network accessed while the ECD is operated in district buildings (including Internet service provided by any commercial service provider).

2. ECDs will not be used to violate the confidentiality or privacy rights of another individual, including but not limited to, taking photographs or audio or video recordings of others without their permission or sharing, posting, or publishing photographs, videos or recordings of others without their permission.

3. Staff is responsible for the personal ECDs they bring to school. The district will not be responsible for loss, theft, damage or destruction of ECDs brought onto district property or to district-sponsored or related events or activities. It should be recognized and understood that a personal ECD may not be compatible with district systems. District support staff will not provide technical support for personal ECDs. Access to district systems with a personal ECD is not guaranteed.

4. Port Townsend Public Schools will not be held liable for commercial service charges that occur from the use of an individual's personal ECD. It is the employee's responsibility to

make sure they understand the usage options that are available to them and whether their provider's service plan includes Internet access and all related costs.

5. Personal ECDs used for district business may be subject to search and seizure.

Network Security and Privacy

1. Users are responsible for maintaining the confidentiality of their user IDs and passwords and will not leave an open file or session which is unattended or unsupervised.

2. Users will not seek information on, obtain copies of, or modify: files, other data, or passwords belonging to other users. Users will also not attempt to misrepresent other users on district technology, nor will they attempt to gain unauthorized access to any data or entity on specific computers or the network.

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

4. Users will avoid using easily-guessed passwords and should change passwords periodically to maintain security.

5. Users will not share their passwords with students.

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.

- 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;

- 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;

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

- 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;

- 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

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

No Expectation of Privacy

It is the policy of Port Townsend Public Schools that district technology is to be used for district-related purposes. Employees have no expectation of privacy when utilizing district technology or when conducting district business using personal ECDs or accounts.

When responding to a public records request under the Washington Public Records Act, the district will access all district technology to provide a complete response. In addition, the district may access personal ECDs if the employee has used a personal device, personal email account or personal social media account to conduct district business. The district may also require employees to conduct searches of such devices and accounts.

The district reserves the right to inspect, without notice, to review, monitor, and log, as appropriate, all activity using district technology when:

1. It is considered necessary to maintain or protect the integrity, security or functionality of district or other computer resources to protect the district from liability;

2. There is reason to believe that the users have violated district policies or procedures;

3. An account appears to be engaged in unusual or unusually excessive activity; and

4. It is otherwise required or permitted by law. Additionally, the username and computing services of the individuals involved may be suspended during any investigation or misuse of computer resources.

District Responsibilities

Port Townsend Public Schools will:

1. Review, monitor, and log, as appropriate, all activity on district technology for responsible use consistent with the terms of district policies and procedures.

2. Make determinations on whether specific uses of district technology are consistent with district policies and procedures.

3. Remove a user's access to district technology, with or without notice, at any time the district suspects that the user is engaged in unauthorized activity or violating district policies or procedures. In addition, further disciplinary or corrective action(s) may be imposed for such for violations.

4. Cooperate fully with law enforcement investigation(s) concerning, or relating to, any suspected or alleged inappropriate activities on district technology or any other electronic media.

5. From time to time, the district will make a determination on whether specific uses of district technology are consistent with the regulations stated above. Under prescribed circumstances, non-student or non-staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district and is authorized by a district administrator.

Discipline and Consequences for Unauthorized Use of Technology

Violation of Port Townsend Public Schools' expectations for use of technology may be cause for disciplinary action up to, and including, termination of employment

Date: 2/21/19

PORT TOWNSEND SCHOOL DISTRICT NO. 50