

ACCEPTABLE USE OF PSESD ELECTRONIC COMMUNICATIONS SYSTEM

Puget Sound ESD maintains an electronic communications system to provide resources for staff, volunteers, students and visitors to communicate, learn, and to access and publish information that enhances the delivery of services to our clients and to the public. Puget Sound ESD grants access to the system for educational and program support activities under the limitations contained in this and related policies. Staff, volunteers, interns and visitors must never use the communications system for any purpose that would violate PSESD policy, the law or that would conflict with the *PSESD Principles that Guide our Culture* as an Anti-racist, Multi-cultural organization.

Applicability & Limitations

- **System Description:** The components of the electronic communications system include, but are not limited to: the wired and wireless computer network and subsystems; Internet access; servers and computer workstations, including stipend-supported mobile devices (e.g., phones, tablets;) telephones, facsimile (FAX;) printers, copiers and scanners; resources to which the system provides access (e.g., file storage, email, databases, Internet-accessible services.)
- **Applicability:** This policy applies *devices owned by PSESD and devices supported by PSESD stipends* at all times and wherever the device is used.
- **No expectation of privacy:** Users of the electronic communications system have no reasonable right to expect privacy. The Superintendent or A designee may access employee electronic communications system accounts without prior notice or approval for business or investigatory purposes. Electronic communications system uses are recorded and are subject to public records disclosure and other legal discovery processes.
- **Filtered Internet:** Users are subject to limited access to the Internet. Web filtering software prevents access a variety of objectionable websites, particularly those that the Child Internet Protection Act requires to be inaccessible (see Internet Safety Policy 50XX/30XX). The Superintendent or a designee may authorize the disabling of such measures for staff, volunteers, interns and visitors engaged in bona fide research or other lawful purposes.
- **Limited personal use:** Personal use of the electronic communications system must not interfere with normal ESD activities or operations, including staff responsibilities and duties, and must incur only negligible cost to PSESD (*de minimus* use.)
- **Access revocability:** Access to the electronic communications system is a privilege and may be revoked by the superintendent or a designee at any time.
- **Professional behavior standards:** The same professional conduct and standards expected of staff are expected when using the electronic communications system. Violation of these standards may be grounds for disciplinary action.
- **Notification & assurance:** All users must agree to abide by this policy before access to the electronic communications system will be allowed. This policy will be posted in all public areas at PSESD facilities and will be presented to guest users of the wireless network as part of their authentication process.
- **Reasonable care of property:** All users will take reasonable care of PSESD physical and intellectual property while connected to its electronic communications systems. Special care

must be given to the security of data and other information regarding the PSESD, its clients and partners.

Expressly Prohibited Uses

- 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, violent, racist, sexist or other offensive, objectionable, 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 user in either public or private messages
- Unauthorized access to the communications system, another individual's account or a restricted account
- Sharing communications systems (e.g., network, computer, website) passwords with any unauthorized individual.
- Malicious or unauthorized use of the system

Adopted: July 2007

Revised: November 2010

Revised: June 2012

Revised: March 2014

Relevant PSESD Board Governance Policies: EL 4, Treatment of Staff
EL 9, Asset Protection

Cross References: Operating Policy No. 5291, Email/Internet Use
Operating Policy No. 5292, Electronic Information Security and Retention
Operating Policy No. 5393, Staff and Student Internet Safety
Operating Policy No. 5294, Staff Use of Social Media

Legal References: RCW 28A.300.285, Harassment, intimidation, and bullying prevention policies and procedures — Model policy and procedure — Training materials — Posting on web site — Rules — Advisory committee
RCW 28A.640.020, Regulations, guidelines to eliminate discrimination — Scope — Sexual harassment policies.
WAC 392-190-058, Sexual harassment—Procedures.
WAC 392-190-060, Compliance—Local school district—Designation of responsible employee—Notification.
WAC 292-110-010, Use of state resources.
47 C.F.R. 54 Subpart F