## SECTION 3.39.1 Student Internet Safety and Responsible Use

**These regulations and procedures provide students and parents in the Poway Unified School District with information about the privileges and responsibilities of using the Internet and District computer networks and resources. In accordance with the Children's Internet Protection Act, the use of PUSD computer systems either at school or away from school requires the following agreement to be read and signed by the student and parent/guardian. It becomes a legally binding agreement when signed (Form PUSD LSS-SIG).**

**I. Educational Purpose: The PUSD Internet system has been established for a limited educational purpose. "Educational purpose" includes classroom activities, continuing education, professional or career development, and high-quality, educationally enriching personal research. It has not been established as a public access service, a public forum, or for political lobbying. District access to the Internet may not be used for commercial purposes. "Commercial purposes" refers to the unauthorized offering, providing, or purchasing of products or services through the District Internet system.**

**II. Responsibilities: While it is impossible to control all material on a public network, the PUSD has taken reasonable precautions to restrict access to materials it considers harmful and to materials that do not support approved educational objectives. Harmful material refers to content that, "taken as a whole by the average person applying contemporary statewide standards, describes in a patently offensive way material which lacks serious literacy, artistic, political, or scientific value for minors." (See Section IV below.) (California Penal Code Section 313-313.5)**

**Teachers and/or staff will instruct students in appropriate ways to access Internet resources. Teachers and/or staff will use reasonable measures to ensure that information gathered from the Internet appropriately supports educational purposes.**

**III. Revocable Right: The use of the PUSD computer system is a revocable privilege for all users. The PUSD computer systems, equipment, and all user accounts are the property of PUSD. Privacy rights do not apply to the use of the computer system or user accounts, and the District reserves the right to monitor and access information maintained in the system and in users' accounts for the purpose of determining if a violation of this agreement has occurred.**

**IV. Prohibited Use: Purposeful access, downloading, or transmission of any "harmful matter" in violation of any federal law, state law, or District policy is prohibited. This includes, but is not limited to:**

- **any information that violates or infringes upon the rights of any other person, including cyberbullying.**
- **any hate-motivated, fraudulent, defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal language or material.**
- **any information or communication that encourages the illegal use of controlled substances, or promotes criminal behavior.**

- **any material that violates copyright laws (Administrative Procedure 6.70.7 – Copyright Material).**
- **transmission, creation, or participation in unauthorized advertisements, solicitations, commercial activities, or political lobbying.**
- **vandalism, unauthorized access, "hacking," or tampering with hardware or software. This includes the introduction of "viruses," "worms," non-licensed or pirated software, or any software or hardware for the purpose of disrupting or damaging PUSD computer systems. (California Penal Code Section 502)**

**All outgoing transmissions of information are unsecured and sent at the risk of the user. The District will remove any information from the system that the staff determines to be unlawful, obscene, pornographic, abusive, harassing, or otherwise in violation of this agreement, including all items defined as "harmful matter." Staff will refer for disciplinary action any individual who violates provisions of this agreement. Cancellation of user privileges and other consequences will be at the discretion of the staff.**

V. **Network Protocols: The use of District computer systems requires that students abide by accepted rules of network behavior. These include, but are not limited to, the following:**

- ***Be polite*. Do not send abusive messages to anyone.**
- ***Use appropriate language*. Do not swear or use vulgarities or any other inappropriate language. Any reference to illegal activities is strictly forbidden. Knowledge of messages relating to or supporting illegal activities must be reported to appropriate authorities.**
- ***Maintain privacy*. Do not reveal either your personal information or that of others. This includes addresses and phone numbers. Before identifying a student by name or photo, the school must have on file an Internet Use Permission form signed by the parent authorizing publication (Form PUSD LSS-SIG).**
- ***Respect copyright*. All intellectual property accessible via the network should be assumed to be the property of the author and may not be reused without his/her permission.**
- ***Do not disrupt the network*. Do not use the network in a way that would disrupt its use by others.**

VI. **Rights and Expectations: The District Internet system is considered a limited public forum, and the District may restrict student speech for valid educational reasons.**

**Students own the copyright to works that are created in school or for class assignments. If the work is created jointly, each student will have joint ownership of the copyright. Additionally, each student and parent/guardian must agree to the posting of work on a District website (Form PUSD LSS-SIG).**

VII. **Security: If a student becomes aware of a security issue or breach on the District computer system, it is his/her responsibility to notify a staff member immediately, either in person, in writing, or via the network system. Sharing details of a security issue or breach with non-staff members is a violation of this procedure and may result in the denial of access or other consequence.**

VIII. **Vandalism: Vandalism of a District computer system and/or hand-held devices will result in cancellation of privileges and/or disciplinary action that may include notification of law enforcement. Vandalism includes, but is not limited to, the uploading or creation of**

**computer viruses or similar software, and the hacking or altering of software or hardware configurations. Parents or guardians may be held financially responsible for any harm resulting from their child's misuse of the computer system.**

**IX. Use of Personal Devices: All students who bring a personal device to a District school site may attach to the Guest District wireless network for Internet access only. No personal devices may be attached by hard wire to the District network. All the rules and regulations stated in the District Technology Use Agreement are still in effect for all network connections.**

**The District is not responsible for lost, damaged, or stolen personal devices. With the permission of the parent/guardian, the District may provide the use of District-owned applications installed by District IT personnel on personal devices. The District is not responsible for personal device performance if the District-owned application is installed on a personal device. The student/parent/guardian agrees to bring in their personal device upon the request of the District, or upon separation from the District, to remove the application for redistribution.**

**Limitation of Liability: The PUSD does not guarantee that functions or services provided through the District Internet service will be without error. The District will not be held responsible for loss of data. Students are responsible for backing up student-generated files. The PUSD specifically denies any responsibility for the accuracy or quality of information obtained via the District computer system.**

**IMPORTANT NOTICE**

**Inappropriate use may result in the cancellation of network privileges. The site system administrator(s) or District security administrator may close an account at any time deemed necessary. Depending on the seriousness of the offense, any combination of the following policies/procedures will be enforced: Educational code, Penal code, District procedures, and school site discipline/network use policy. The disciplinary action may include, but is not limited to, discipline conferences, suspension, expulsion, and possible financial restitution.**