The Preuss School UC San Diego

The Preuss School UC San Diego

Dr. Helen Griffith
Executive Director

Dr. Matthew Steitz
Principal

Policy: Scholar Device / Network / Internet Acceptable Use Policy | S1005 Acceptable Use Policy

Purpose of Policy:

Every Preuss School user should act in an ethical and legal manner consistent with school goals and objectives and should conform to educationally appropriate use and network etiquette that includes being polite, using appropriate language, respecting the privacy of others, and respecting the computer equipment.

Users of The Preuss School network services should remember that the level of confidentiality on school-owned computers may not be the same as that expected when using their own equipment or Internet services. Electronic communications*, files, and other Internet records may be examined for educational and administrative purposes and to verify that acceptable-use guidelines are being followed. (*For purposes of this document, electronic communications include but are not limited to e-mail, chat, blogging, Internet posting, and instant messaging.)

The Preuss School has taken reasonable steps to ensure student safety with the use of a variety of software tools. Web filtering software is used to block out unwanted and inappropriate content. Device management software is used to monitor on-task behaviors in the classroom. Content monitoring software is used to alert school administration to issues of bullying, online predators, sexual content and more. Because the Internet contains an unregulated collection of resources, even with safeguards in place, the school cannot guarantee the accuracy of the information or the appropriateness of any material that a student may encounter. The Preuss School believes that the benefits of Internet access in the form of information resources and opportunities for collaboration far exceed any disadvantages. Before using the school's network resources, each student and his/her/they parent/guardian shall sign and return an Acceptable Use Agreement (Network Responsibility Contract), which shall specify user obligations and responsibilities and shall indemnify the school for any damages. This document will be shared in the Opening Of School packet. The parent/guardian shall agree not to hold the school responsible for materials acquired by the student on the system, for violations of copyright restrictions, users' mistakes or negligence, or any costs incurred by users.

Ultimately, parent(s) and guardian(s) of minors are responsible for setting and conveying the standards that their child should follow. Use of the school's devices, network, or the Internet is a privilege that may be revoked at any time for inappropriate conduct. Internet and network use should be strictly limited to educational purposes.

Content of S1005 Acceptable Use Policy:

Acceptable use policy

As a user of The Preuss School network and Internet connection, I agree to:

- Use electronic resources and communications for educational purposes only.
- User accounts are to be accessed only by the authorized user of the account and for school purposes only. Account users are ultimately responsible for all activity under their account.

- Use my network access in an acceptable manner, follow all school rules and regulations regarding network use, including being polite, using appropriate language and respecting others' privacy.
- Scholars are responsible for the appropriateness and content of material they transmit or publish on the system.
- Use online time and other network resources efficiently.
- Assist in keeping The Preuss School network free from virus attacks by refraining from opening attachments and running files from unknown or potentially malicious sources.
- Be respectful to all computers and computing equipment owned by The Preuss School and report any physical tampering with devices by any other users.
- Do not damage the computers by carrying them by the screen, pulling off keyboard keys, having open containers of liquid or food near the laptops.

Inappropriate online conduct includes, but is not limited to:

- Using the network for illegal activities, including unauthorized installation, use, storage, or distribution of copyrighted software or materials in violation of copyright laws.
- Using the network for private business or commercial enterprise.
- Using the network for political activities.
- Use of another individual's name or account.
- Allowing another user access to your account.
- Sharing electronic account passwords, leaving passwords available in obvious locations, or leaving "signed on" computers unattended.
- Disclosing, using, or disseminating personal identification information about oneself or others when using electronic communication. Scholars are also cautioned not to disclose such information by other means to individuals located through the Internet without the permission of their parents/guardians. Personal information includes the student's name, address, telephone number, Social Security number, or other individually identifiable information.
- Reading other users' electronic mail or files.
- Attempting to interfere with other users' ability to send or receive electronic mail, or deleting, copying, modifying, or forging other users' mail.
- Distributing electronic media in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system (e.g., using torrent software, downloading large files; sending mass electronic messages; downloading video and audio files not directly related to school goals, excessive chat or instant message use for non-educational purposes).
- Intentionally uploading, downloading, distributing, or creating computer viruses.
- Attempting to vandalize, harm, tamper with or destroy school equipment, data, or materials.
- Manipulating the data of any other user.
- Unauthorized access to servers, computer systems, or network equipment.
- Tampering with the computer (monitors, keyboards, mice, cables, etc.) or network hardware (network cables or wall jack) in order to diminish or damage functionality.
- Using electronic resources and communication other than educational purposes.
- Using proxy servers, virtual private networks (VPN), websites, or software to bypass network filters.

Cyber-bullying
The Preuss School UC San Diego's policy on the prevention of "cyberbullying" is aligned with the CA ED Code, SDUSD, and the Anti-Defamation League guidelines. Cyberbullying is broadly defined as the "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices. The Preuss School identifies the following as forms of "cyberbullying" offenses as prohibited behaviors for student conduct in cyberspace:

- Accessing, posting, submitting, publishing, or displaying harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability, religion or political beliefs. California Penal Code Section 313(a)
- Trolling, flaming, impersonation, trickery, or e-bullying on forums, e-mail, or websites including but not limited to myspace.com, facebook.com, youtube.com.
- Sending or exchanging messages that are inconsistent with school or school policies.

In the event a Scholar violates any part of the *AUP and/or Technology Acceptable Use Student Agreement*, misuse electronic resources, or violate state or federal laws, consequences will be imposed by the school consistent with Student Handbook policies. Each situation will be considered independently and consequences will range from a discussion about the rules and expectations regarding usage and/or a complete withdrawal of access to all computer technology in accordance with the Restorative Responses and Preventative Practices section of the Scholar Handbook. We support the parent's or guardian's right to authorize or decline Internet access for their student.