Internet Safety Policy

Computers, and internet access while in the school building, will be available to qualifying students at Promontory School. Promontory's goal is to provide these services to students in order to promote "Great Thinkers" by facilitating resource sharing, innovation, and communication.

It is the policy of Promontory School to (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Technology Protection Measures

Student use of computers must be in support of education and research and must be consistent with educational objectives of Promontory School. Accordingly, internet access at Promontory is filtered and monitored on an ongoing basis. This is to protect against access by adults and minors to visual depictions that are obscene, pornographic, or harmful to minors. Filtering may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes upon receiving special permission from the Director. Additionally, Promontory devices that may be assigned or checked out to students for home use will also be filtered and monitored on an ongoing basis to protect students as outlined above.

To the extent practical, steps shall be taken to promote the safety and security of users of the Promontory School online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Documentation of technology protection measures will be retained for at least five years after the last day of the funding year in which the measures were relied upon to obtain E-Rate funding..

Internet Safety Policy

Students will be educated in appropriate online behavior, including cyberbullying awareness and response and interacting with other individuals on social networking websites and in chat rooms. The safety and security of students when using electronic mail, chat rooms, and other forms of direct electronic communications is a priority at Promontory; As such:

1. Students will sign computer use and safety agreements annually.

2. Students are strictly prohibited from:

> • accessing or creating files or materials without authorization.
>
> • attempting to hack into any school systems.
>
> • accessing or creating offensive, profane, or pornographic files.
>
> • plagiarizing works or violating copyrights or trademarks.
>
> • attempting to bypass computer security.
>
> • Having food or drinks near computers.

3. There will not be an expectation of privacy in files, disks, documents, internet history, etc., which have been used or created with Promontory equipment.

4. All documents, files, and folders created with school hardware/software remain the intellectual property of Promontory School.

5. Vandalism will result in appropriate disciplinary action. Vandalism includes, but is not limited to,: abusive overloading of data on the server, creating or uploading/downloading computer viruses, or any malicious attempt to harm or destroy the property.

6. Security is a high priority. Students must use their own login credentials and are prohibited from using another individual's account or login information at any time. Any security concerns must be reported to the teacher/supervisor, director, or system administrator.

7. Personal information is restricted, password protected, and stored only on the school servers. Only authorized personnel have access to student information. Teachers will sign disclosures regarding the use and dissemination of personal student information. Promontory staff may use only software programs approved by the Promontory technology team to supplement student learning. Promontory shall follow current federal and state law in the sharing of student information with such software vendors.

8. The use of the computers and internet is a privilege, not a right. Inappropriate use of these resources may result in disciplinary action, including the possibility of suspension or expulsion and/or referral to legal authorities. The teacher/supervisor, director, or systems administrator may limit, suspend, or revoke access to electronic resources at any time.

9. Users are liable for any misuse of the systems.

10. Parents may opt out of the publication of student work and photos.

Documentation of the Internet Safety Policy will be retained for at least 5 years after the last day of the funding year in which the policy was relied upon to obtain E-Rate funding.