ACCEPTABLE USE POLICY

California Pacific Charter Schools and its programs ("CalPac" or the "Charter School") provides technology resources to its students solely for educational purposes. Through technology, CalPac provides access for students and staff to unlimited resources. Expanding technologies provide tremendous opportunities for enhancing, extending, and rethinking the learning process. The goal in providing these resources is to promote educational excellence by facilitating resource sharing, innovation, and communication with the support and supervision of the parent and credentialed teacher. With this access brings the potential exposure to material that may not hold educational value, or may be harmful or disruptive to the student's learning experience.

The purpose of this policy is to ensure that student internet access on school owned computers will be appropriate and used only for educational purposes, consistent with the acceptable standards of the school.

All computer equipment, programs, supporting materials, and peripherals of any nature which the student receives from the school are loaned to the student for educational purposes only and belong to the school. As a condition of receiving and using any such equipment, the student and student's parents acknowledge that there is no right of or expectation of privacy whatsoever related to the student's use of such equipment. The school retains the right to monitor, at all times, Internet/computer activity accessed by this equipment, review any material stored in files on such equipment, edit or remove any material which the school staff, in its sole discretion, believes violates the above standards, and terminate the Internet/Computer Agreement of any persons violating the conditions set forth in this policy.

Information services such as online educational resources provided by the Charter School may occasionally require new registration and account information to continue the service. This will require the School to give out certain portions of student's personal information to one or more 3rd party vendor(s) required for this requested service, such as logon information, etc. Student and parent's signatures of this policy and use of said computer equipment or school-provided online resources indicate specific consent to such release of personal information.

Students using the Internet shall be closely supervised by the parent. Students and their parents are ultimately responsible for the materials accessed through the use of student Internet accounts. Parents or guardians will be responsible for the supervision of students using the internet.

ACCEPTABLE USE POLICY

The California Computer Crime Bill (1979) added section 502 to the Penal Code making it a felony to intentionally access any computer or system or network for certain purposes, including:

1) Devising or executing any scheme or artifice to defraud or extort or,
2) Wrongfully control or obtain money, property, or data.
3) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
4) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network
5) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.
Anyone committing acts of this kind, or any other actions prohibited by law with school owned computers and/or equipment will face legal action and disciplinary procedures.

It is the intent of this policy to protect students from inappropriate information. However, the staff cannot screen all of the materials available on the Internet. Willful access to inappropriate material in any form by students as well as the importation of any material from "outside sources" on school owned computers and/or equipment is a violation of this policy and may result in disciplinary action including, but not limited to, the revocation of School-provided computer and/or equipment and/or discipline, up to and including, expulsion of the student. Students, staff and parents hold a joint responsibility to insure that inappropriate material is not displayed or available on any computer.

Parents/guardians will teach the student about Internet safety, including how to protect online privacy and how to avoid online predators using resources such as materials available at: http://www.digitalcitizenship.net. CalPac has also adopted internet safety policies in accordance with applicable law, including the Children's Internet Protection Act, which will be provided to parents/guardians.

This policy does not attempt to articulate all required or proscribed behavior by users. Misuse may come in many forms; it is commonly viewed as any transmission(s) sent or received that suggest or indicate pornography, unethical or illegal solicitation, racism, sexism and inappropriate language.

The following characterize, but do not exhaustively list all unacceptable behavior:

1) Using the school funded Internet/computer system for illegal, inappropriate, or obscene purposes or in support of such activities
2) Utilizing the school funded Internet/computer system for any illegal activity including violation of copyrights or other contracts relating to licensed uses.
3) Intentionally disrupting equipment of system performance.
4) Downgrading the equipment or system performance.
5) Damaging or misusing any hardware or software.
6) Utilizing the school's computing resources for commercial/financial gain or fraud.
7) Pirating and/or theft of data, equipment, or intellectual property.
8) Gaining or seeking to gain unauthorized access to resources or entities.
9) Utilizing the system to encourage the use of drugs, alcohol or tobacco or any promotion or attempt to promote any unethical behavior.
10) Using harassing, abusive or obscene language.
11) Annoying, harassing or intentionally offending another person.
12) Introducing computer viruses into the system.
13) Forging electronic mail messages or using an access owned by, or used by another.
14) Wasting of resources.
15) Invading the privacy of others.
16) Possessing data in any form (including hard copy or disk) which might be considered a violation of these rules.

Consequences of non-compliance

As with any other violation of school rules and regulations, consequences of violations include, but are not limited to, the following:

1) Suspension of school funded Internet access
2) Revocation of school funded Internet access
3) Limitations of school funded computer access
4) Revocation of school funded computer access
5) Disciplinary processes up to expulsion or involuntary withdrawal
6) Legal action and prosecution
7) Financial liability for loss of Internet/computer system

The parent/guardian is responsible to abide by and to ensure the student abides by the provisions and conditions of this policy and that any violations of the above provisions may result in disciplinary action, the revoking of the user account, and appropriate legal action.

The parent/guardian is also responsible to report any misuse of the information system to school administration. All the rules of conduct described in the publication entitled "Internet/Computer Acceptable Use Regulations" apply when on the Internet or using the school-owned computer.