## PPEC Technology and Computer Use Policy

Our commitment to 21st-century learning is supported through the possibility of age-appropriate use of our laptops available to teachers and students to enhance their experience while at PPEC. Activities can vary from viewing information and interacting with safe, online exercises to researching, producing and publishing work.

Each family was given the right to accept or deny the Acceptable Use Policy through the D49 enrollment process.

Student Computer Use Absolutes at PPEC:

- Always log off your computer
- Know how to log into the firewall
- Plug in your laptop when finished for the day

### Network Netiquette

PPEC students are expected to follow the rules of network etiquette or "netiquette". The word "netiquette" refers to common-sense guidelines for conversing with others online. Students are encouraged to abide by these standards:

- Establish Instant message usernames and email addresses appropriate for the school setting.
- Avoid sarcasm, jargon, and slang. Swear words are unacceptable.
- Avoid using abbreviations, texting language or inappropriate contractions. When students type these abbreviations, they are telling everyone they cannot type well enough to use complete words.
  - Example:

Appropriate	Inappropriate
"you"	"u"
"your"	"ur"
"see you later"	"с уа"

- Never use derogatory comments, including those regarding race, age, gender, sexual orientation, religion, ability, political persuasion, body type, physical or mental health, or access issues.
- Focus your responses on the questions or issues being discussed, not on the individuals involved.
- Be constructive with your criticism, not hurtful.
- Review your messages before sending them. Remove easily misinterpreted language and proofread for typos.
- Respect other people's privacy. Do not broadcast online discussions, and never reveal other people's email addresses.

# Internet Safety

Students must not reveal personal information about themselves or other persons on the internet. For example, a student should not reveal his/her name, home address, telephone number, or display photographs of him/herself or others to persons outside of PPEC.

Students cannot agree to meet in person anyone they have met only on the Internet and who is not affiliated with PPEC.

# Internet Safety Websites

#### The following sites are recommended by the **Colorado Department of Education** for parents:

<u>ConnectSafely.org</u> is the leading interactive resource on the Web for parents, teens, educators – everyone engaged and interested in youth safety – on the fixed and mobile social Web.

<u>GetNetWise.org</u> is a public service from Internet industry corporations and public interest organizations to help ensure Internet users have safe, constructive, and educational or entertaining online experiences.

<u>iKeepSafe.org</u> tracks global trends and issues surrounding digitally connected products and their effect on children. This research drives the continuous creation of positive resources for parents, educators, and policymakers who teach youths how to use new media devices and platforms in safe and healthy ways.

<u>NetSmartz.org</u> is an interactive, educational program of the National Center for Missing & Exploited Children® (NCMEC) providing age-appropriate resources to help teach children how to be safer on- and offline. The program is designed for children ages 5-17, parents and guardians, educators, and law enforcement.

<u>Family Online Safety Institute</u> is an international, non-profit organization which works to make the online world safer for kids and their families.

Understanding A Child's Virtual World: (<u>English</u>/<u>Spanish</u>)- A handbook for parents and guardians.

<u>Compliance and Safety</u> offers a comprehensive internet safety tip resource.

### Accountability

Posting anonymous messages are not permitted unless authorized by the course's online teacher. Impersonating another person is strictly prohibited.

- Each student shall only use their own username and password and shall not share these with anyone.
- Students shall log into Class Connect Sessions with first name and last initial only.
- Students may not interfere with a student's ability to access PPEC, e.g., disclosing their password or using someone else's user account. Each student is responsible for any and all activity associated with their usernames and passwords.
- Students are encouraged to change their password(s) frequently, at least once per semester or course.
- Students shall not publicly post their personal contact information, e.g., address,

phone number or anyone else's.

- Students shall not publicly post any messages sent to them privately.
- Students shall not download, transmit or post material intended for personal gain or profit, non-PPEC commercial activities, non-PPEC product advertising, or political lobbying on a PPEC owned instructional computing resource.
- Students may not use PPEC instructional computing resources to sell or purchase any illegal items or substances.
- Students shall not upload or post any software on PPEC instructional computing resources not specifically required and approved for student assignments.
- Students may not post any MP3 files, compressed video, or other non-instructional files to any PPEC server.