

# PETCHS Student Acceptable Use Policy

## Overview

The school provides students with access to computers in designated computer labs throughout our building. Through these labs, whether wired or wireless, students have access to network resources, software applications and the World Wide Web. The technology we provide is intended to advance the students educational experience, as well as assist with meeting educational goals and standards. Students should only use assigned computers in labs, and never a staff member's computer. Also, under no circumstances should students share their account information with anyone.

The technology we provide is a privilege, not a right. Therefore, before a student can utilize our resources, the students as well as a parent or legal guardian, must read and sign our Acceptable Use Policy (AUP). In this document, we aim to educate the user on the school's expectations and the responsibilities of the user.

## Expectations

Our students are expected to abide by the policies set forth in this document. AUP violations can cause serious academic consequences for a student. If you lose your computer privileges due to a violation, you may not use a PE & T computer at any time during the duration of the disciplinary action imposed. The violation is not the teacher's responsibility; the student is expected to be held fully responsible for his or her own actions. We provide 3 options for students who violate our AUP:

- Provided the means is available, you can complete computer-related assignments after-school at home, a public library, etc, not on school grounds.
- A student can recommend to his or her teacher another way to complete the assignment. This is the student's responsibility to create the alternative assignment. The teacher will use their own discretion as to whether or not the proposal is acceptable in accordance with the original assignment.
- If no valid alternatives can be found, the end result may be that the student fails the course.

## **Level One Violation Descriptions and Disciplinary Actions**

Level One Violations are considered minor offenses, and usually have little effect on other users or resources. These violations include, but are not limited to:

- Using technology during class for non-class related reasons (games, videos, music files, CDs, DVDs, browsing off-topic websites)
- Running unauthorized programs. In this case, these programs are those that pose no threat to network or data security
- Instant messaging or emailing during class without teacher authorization through technologies including, but not limited to: instant messenger, 3rd party or school email systems, ICQ, etc
- Using our technology for any other purpose besides school related activity
- Accessing or attempting to access chat-rooms, message boards, news groups or any messaging related system unless authorized by your teacher
- Removing or replacing hardware or cables without authorization
- Forgotten Passwords. Students will be provided their passwords during their initial use of our computers. After this, it is their responsibility to keep track of their own passwords
- Food and Drink. Students should never have any type of food, snack or drink in areas designated as a computer lab. Since these items are not allowed outside of the cafeteria anyway, this would cause the student to be written up twice; once for the AUP violation, and once for the Discipline Code violation

### **Disciplinary Actions for Level One Violations:**

- 1st Offense: Loss of PC privileges for remainder of day; 1 demerit; 1 detention
- 2nd Offense: Loss of PC privileges for 1 week; 5 demerits; 5 detentions
- 3rd Offense: Loss of PC privileges for 1 month; 10 demerits; 10 detentions

After 3rd Level One Violation, all subsequent Level One Violations become Level Two Violations

## **Level Two Violation Descriptions and Disciplinary Actions**

Level Two Violations are considered major offenses, and typically show the students disregard for other users, the school's equipment and our policy.

These violations include, but are not limited to:

- Banned website access attempts or actual visits. A list of all sites a student accesses or attempts to access is recorded in accordance with the Children's Internet Protection Act (CIPA). Our proxy servers automatically pick up any illegal site requests from students. Students are accountable for accessing, or attempting to access illegal sites unless approved by their teacher. Illegal sites include, but are not limited to: adult oriented sites, gambling sites, illegal drug sites, gaming or arcade sites, social networking sites (myspace), etc. For this violation, parents or guardians will be sent a list of sites their child accessed or attempted to access
- Installing any type of software that has not been approved by your teacher
- Downloading and storing files on the network without teacher permission. These files include, but are not limited to: pictures, music, movies, etc
- Failure to report vandalism or network security violations such as sharing user accounts
- Vandalizing or purposely damaging hardware causing damage less than \$100
- Sharing Your Account with Another Student or Using Another Student's Account
- Using technology to cheat, plagiarize or infringe copyright
- Spamming: a disruptive, esp. commercial message posted on a computer network or sent as e-mail
- Creating documents or posting information aimed at insulting, defaming or belittling another student, faculty, or staff member
- Using or attempting to use any type of proxy or anonymous surfing service to mask internet usage

### **Disciplinary Actions for Level Two Violations:**

- 1st Offense: Loss of PC privileges for 1 week; 5 demerits; 5 detention
- 2nd Offense: Loss of PC privileges for 1 month; 10 demerits; 5 detentions; Parent and student must come in to review the AUP before access is given back to student
- 3rd Offense: Loss of PC privileges for 1 year; 30 demerits; 10 detentions; Student must attend Summer School

After 3rd Level Two Violation, all subsequent Level Two Violations become Level Three Violations

## **Level Three Violation Descriptions and Disciplinary Actions**

Level Three Violations are considered severe offenses, and are typically malicious in nature with the intent to cause a major disruption on our network, or within the classroom.

These violations include, but are not limited to:

- Using a staff account to access network resources (software, typing papers, printing, etc) or surf the internet. This is under NO CIRCUMSTANCES allowed at any time
- Using a Staff PC. This is under NO CIRCUMSTANCES allowed at any time. We have designated areas for students to use computers, a staff member's PC is never OK to use
- Attempting to acquire unauthorized access to the PE & T network. This includes trying to steal teacher, staff or administrators passwords
- Using any personal hardware on our network without teacher or administrator consent
- Creating documents or posting information advocating or threatening illegal acts towards self, another student, or staff member
- Attempting or actually using tools for use with hacking, phishing, packet sniffing, etc.
- Setting up meetings with those you met online while at school; gambling; attempting to purchase illegal narcotics, or any other illegal activity
- Purposely and willfully vandalizing or attempting to vandalize software, data or hardware causing damage greater than \$100

### **Disciplinary Actions for Level Three Violations:**

- 1st Offense: Suspension; loss of PC privileges for 1 year; 30 demerits; 10 detentions; Parent must come in to review AUP, and make sure all parties understand the seriousness of this situation. Student must attend Summer School
- 2nd Offense: Expulsion will be recommended to the Discipline Review Board

If at any time a student is caught using a PC during his or her disciplinary period, the student will be immediately charged with a Level 3 Violation.

## Limitation of Liability

- PE & T reserves the right to change at any time violation classifications and types, disciplinary actions, etc.
- PE & T will make every attempt to provide a network that is without defect, but can not make any guarantees that this will hold true
- PE & T will not be considered responsible for any interruptions of computer use for any reason, and/or the loss of data (both saved and unsaved)
- PE & T will not be held responsible for the accuracy of information obtained through or stored on our network, or on our website and PowerSchool system
- PE & T will shift responsibility of financial obligations of damages caused by the unauthorized use of the system to the user who performed such acts

## Consent

By signing below you, the student, are agreeing that you have read and understand this document in its entirety and you agree upon the disciplinary actions set forth in this document if you violate this policy.

Student Printed Name: \_\_\_\_\_

Student Signature: \_\_\_\_\_

Date: \_\_\_\_\_

By signing below, you, the parent or legal guardian of the student signing above, are granting permission for your son or daughter to use school networked computers. With your signature, you are agreeing that you have read and understand the above stated document in its entirety, and you agree upon the disciplinary actions set forth in this document if your child violates this policy.

Parent/Guardian Printed Name: \_\_\_\_\_

Parent/Guardian Signature: \_\_\_\_\_

Date: \_\_\_\_\_