

Policy on Acceptable Use of Technology for Students, Faculty, Staff and Subcontractors

The use of technology, including the WPC network (PCNet), is a privilege, not a right. Penn Charter regulates access to and use of technology and the network by principles consistent with the Quaker values expressed in the school's philosophy: values that include honesty, the individual's responsibility to the community, and the respectful treatment of every person. Thus, technology users are expected and required to avoid actions that are dishonest, unkind (such as personal attacks and invasion of privacy), invasive, illegal (such as libel, slander, vandalism, sexual harassment, theft, unauthorized access), or in other ways inappropriate.

The purpose of this policy is to outline the guidelines and responsibilities of students, faculty, staff and subcontractors using technology at the William Penn Charter School (WPCS).

The guidelines and prohibited actions described in this policy apply to any use of the Penn Charter network (PCNet) to interact with any social networking website including, but not limited to, Myspace.com and Facebook.com. In addition, use of technology, including PCNet, in negative or derogatory ways may be in violation of other Penn Charter policies and rules of conduct including, but not limited to, the Harassment, Off-Campus Behavior, and/or Alcohol and Other Drug policies.

Permitted Use of Technology

The use of the school's technology resources is for academic and school-related purposes only.

Portable electronic devices, such as CD players, digital players & recorders, personal video cameras, DVD players, and electronic games may only be used on campus during the academic day for school-related projects only. In the Upper School, MP3 players may be used by students as long as they are engaged in quiet study (in the library, study hall, computer lab, or the lounges) and are not disturbing others. Students are responsible for knowing and following individual division guidelines. Students maintain the responsibility for properly securing their property

Student cell phones may not be seen or heard in the building during the academic day. Students must follow individual division guidelines outlined in the *Student Handbooks*.

Acceptable Use Policy

Personal Laptops and Other Network-capable Devices

Students may bring their own personal laptops and other electronic devices on campus for use during the school day for academic or school-related purposes only.

All personally-owned laptops and/or other electronic devices, for students, faculty and staff who wish to use PC network, must be registered with the Educational Technology Department and are subject to access, at any time, by School personnel, if needed to insure the safety and security of William Penn Charter students and/or PCNet.

In-class use of student-owned laptops, and other electronic devices is at the discretion of the teacher. As with school-owned computers, Internet and network use is monitored.

The use of personally-owned laptops, and other electronic devices, is governed by the policies outlined in the Penn Charter Student and Faculty *Handbooks*, including the Acceptable Use of Technology Policy.

Students and faculty members who choose to bring personally-owned laptops, as well as other electronic devices, are responsible for the safety and security of those items.

Operating system updates and viable virus protection software must be installed on personally-owned laptops and may be spot-checked at the discretion of the Education Technology Department.

No user may reveal over the Internet, in any form, the personal information of a current or former student, administrator, faculty or staff member, or parent. For specific web publishing guidelines, see the "Web Publishing Guidelines for Safe, Legal and Effective Content," available online in the *Student Handbooks*. Network and email passwords may not be shared.

Students should not access files other than their own unless given permission by either the teacher or administrator.

Great care must be taken when using the network

to communicate since every message sent via PCNet represents you and the school.

Personal issues or inter-personal conflicts should not be handled via e-mail. Assume that e-mail is not confidential, since e-mail you send can be sent to others.

Students MUST receive permission from a faculty member or administrator before sending unsolicited email to a group of more than 20 people.

Prohibited Actions

Slander and Libel: Harmful and false statements will not be tolerated.

Vandalism: Deliberate attempts to damage or alter the hardware, software, or information residing in the school or on the school network or any other computer system attached through the Internet will violate this policy. Vandalism includes, but is not limited to: attempting to violate the integrity of private accounts, files or programs, the deliberate infecting of the network with a computer "virus," attempts at "hacking" into any of the computers using any method, or other such actions will not be tolerated.

Theft/Plagiarism: Users should treat information found electronically the same way they do information found in printed sources. Rules against plagiarism will be enforced. It is the responsibility of each user to comply with the requirements of the owners of the software regarding its acquisition and use. Students, faculty, staff, or subcontractors may not use any Penn Charter technology resource for the illegal copying, storing or disseminating of illegally acquired software/intellectual property. Theft includes identity theft whereby a person unscrupulously impersonates another person online.

Harassment: All forms of harassment in cyber-space, often called cyberbullying, are unacceptable. Cyberbullying includes but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another person by sending or posting inappropriate and hurtful e-mail messages, instant messages, text messages, digital pictures or images, or website postings (including "blogs"). Community members who feel that they have been the victim of such misuses of technology should not erase the offending material from the system. They should print a copy of the material and report the incident immediately to the appropriate division director, Upper School dean of Students, Middle School assistant director, or the director of educational

technology. All reports of harassment in cyberspace will be investigated fully and sanctions may include but are not limited to the loss of computer privileges, detention, suspension, separation, or expulsion from school.

Inappropriate Access: Users may not use the PCNet to access inappropriate or "adult" materials found on the Internet. Users not exercising responsibility by accessing such materials will lose all Penn Charter technology access. Students that inadvertently access inappropriate material are responsible for immediately notifying a faculty or an Educational Technology staff member.

Chain Letters and Other "Spreading" Schemes: Chain letters, pyramid schemes, forwarding or replying to "contests," "fast cash" schemes, mass cross-postings, and uninvited mass mailings are all highly wasteful of network resources and totally forbidden on the Internet and on the Penn Charter network. Users participating in such activities may have their e-mail addresses permanently revoked in accordance with the Internet standards on this matter.

Access Controls and Firewalls: Attempts to subvert or avoid access controls or firewalls is prohibited. Attempting to access blocked sites by other means is also prohibited. Questions about blocked sites should be directed to the Educational Technology department.

School Responsibilities

A system administrator or school administrator may assume access rights to a user's private files and electronic devices, when required for maintenance of the school's technology resources, in emergencies, or in the course of investigating possible policy infractions.

Users found in violation of these guidelines risk disciplinary action, including having network privileges revoked.