

## COMPUTER TECHNOLOGY ACCEPTABLE USE & INTERNET SAFETY

PITTSYLVANIA COUNTY SCHOOLS recognizes the importance of computer technology in providing a relevant and appropriate education. Our goal is to provide students and teachers with access to modern technology in an environment that encourages exploration, individual creativity and educational development. New avenues of learning that offer unique challenges to the staff and students come with the use of modern technology. The new technologies that use global communication networks provide the students and teachers with learning opportunities unavailable just a few years ago. The power of these systems lies in their ease of use and ability to connect instantly to a growing host of global resources. With every new technology there is the potential for productive use and destructive use. It is the responsibility of the user to use the technology appropriately. The use of the technological facilities provided by PITTSYLVANIA COUNTY SCHOOLS to students and faculty is a privilege.

This *Acceptable Use Policy* (AUP) is designed to describe how PITTSYLVANIA COUNTY SCHOOLS expects the technology to be used. **Students violating this policy may suffer disciplinary action including but not limited to the loss of privileges relating to the use of technology in the schools as described in the *Student Conduct* policy (JFC-PC). Employee violations of this policy may result in disciplinary actions up to and including probation or dismissal as described in policies GBM (*Certified Personnel*) and GBMA (*Classified Personnel*).** During the course of the school year, additional rules regarding Internet safety may be added to address emerging technologies. Upon approval by the School Board, any such rules will become part of this *Acceptable Use Policy*.

### **Responsibilities of the Information Technology Department (IT Department)**

The IT Department is responsible for the design, implementation and maintenance of all aspects of the division- wide network infrastructure including the procurement and management of facilities that connect the division's Intranet to the public Internet. The internal systems that route, switch and interconnect the diverse system within the Intranet at both the hardware and software levels are the specific responsibility of the IT department. Funds to support this mission are included in the IT budget. This includes but is not limited to network support of instructional applications not specifically maintained by vendors outside the PITTSYLVANIA COUNTY SCHOOLS (PCS) network. The IT Department supports and maintains the Internet filtering systems, MS exchange server and all other application servers in its Network Operations Center (NOC) server facility.

### **Limited Purpose of Educational Mission**

PITTSYLVANIA COUNTY SCHOOLS provides access to its computer system, including access to the Internet, as a privilege, and not as a right, to its students and staff. PITTSYLVANIA COUNTY SCHOOLS has a limited educational purpose which includes the

(continued)

use of its system for classroom activities, professional or career development, and limited high-quality, self-discovery activities. Users are expected to use Internet access through the computer system to advance educational and personal goals consistent with the mission of PITTSYLVANIA COUNTY SCHOOLS and its policies. **Uses which may be acceptable on a user's private personal account on another system may not be acceptable on this limited purpose system which PITTSYLVANIA COUNTY SCHOOLS provides.**

### **1. Acceptable Uses**

- 1.1. School computer facilities are for the educational and administrative use of students and staff.
- 1.2. The purpose of the division's network infrastructure and the Internet is to support and enhance the educational environment of the schools.

### **2. Communications and E-mail**

- 2.1. Creation or transmission of material in violation of any Commonwealth of Virginia, United States or international regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secrets and is applicable to the use of mobile devices.
- 2.2. Users of a generic school E-mail account or any account not specifically assigned to their name must include their name as part of the E-mail subject line.
- 2.3. Student communication with other Internet users is prohibited unless approved by the supervising teacher. Blogs, forums, or chat rooms should be closely monitored by the supervising teacher.
- 2.4. It is the responsibility of the student user to report to responsible school personnel any knowledge of electronically transmitted attacks made over the Internet or LAN.

### **3. Etiquette**

- 3.1. All communications, whether local over the school network or over the Internet, must be conducted in a polite and considerate manner.
- 3.2. Transmission of derogatory, demeaning, or vulgar material and personal attacks is expressly prohibited.
- 3.3. Any behavior intended to disrupt the use of computer facilities is prohibited.
- 3.4. Using profanity or language that may be offensive to others is prohibited.
- 3.5. All anonymous correspondence is prohibited.

### **4. Activities Prohibited Using School Telecommunications Facilities**

- 4.1. Any use by staff that infringes upon contractual duties is prohibited.
- 4.2. Unauthorized use of credit cards, debit cards, or any other conveyance of financial resources to secure access to services or to purchase products is prohibited.
- 4.3. Use for product advertising or for political purposes is prohibited.
- 4.4. Unauthorized remote access to school facilities via telecommunications facilities is prohibited.

(continued)

- 4.5. Using the division's network facilities for financial gain, commercial activity, or any illegal activity is prohibited.
- 4.6. Any activity that results in the loss of another person's privacy is prohibited. This includes, but is not limited to, copying software or data files containing personal, private, or confidential employee information for the purpose of electronic or physical removal from school grounds.
- 4.7. Using, viewing, transmitting, or attempting to locate material that is unacceptable in a school setting is prohibited. This includes, but is not limited to, pornographic, obscene, violent, or vulgar images, sounds, music, language, video or other materials not in keeping with the educational mission of PITTSYLVANIA COUNTY SCHOOLS.

## **5. Access to Computer Facilities**

- 5.1. Students are prohibited from entering restricted areas without permission of the staff and without adult supervision. Such areas include, but are not limited to, administrative work areas, server rooms, wiring closets, labs, and classrooms.
- 5.2. Removal of equipment from the school premises or relocation of equipment within the school is prohibited unless approved through the office of the Assistant Superintendent for Information Technology. Inventory of equipment, network monitoring, and logging of Internet access are based on network addressing and location within the school.

## **6. Software**

- 6.1. Copying commercial software in violation of copyright laws is prohibited.
- 6.2. Installing, copying or executing software not licensed by PITTSYLVANIA COUNTY SCHOOLS is prohibited.
- 6.3. Unlawful possession of software licensed to PCS is strictly prohibited.
- 6.4. Software and/or equipment distributed by PCS for home use is restricted to use by PCS employees or students as specified in the license agreement.

## **7. System Use**

- 7.1. Students and staff are expected to use the computer equipment and network infrastructure in the manner provided without alteration.
- 7.2. Any use of computer facilities which disrupts the educational environment of the school is prohibited.
- 7.3. Damaging, marring, or defacing computer hardware in any manner is prohibited. Computer hardware refers to the monitor, CPU, keyboard, mouse, printer, and any associated equipment. Computer hardware also includes network infrastructure such as cables, connections, switches, or electrical facilities.
- 7.4. Deleting, altering or modifying software residing on school equipment is strictly prohibited. This includes modifying workstation configurations or network security settings.
- 7.5. Possession or use of hacker utilities designed to circumvent security systems or gain unauthorized access to computer facilities is prohibited.

(continued)

- 7.6. All Internet access at the school level must be through the School Board's Internet filtering system that provides filtered, monitored and logged Internet service. Access to the Internet via other connections is strictly prohibited unless a waiver is provided by the office of the Assistant Superintendent for Information Technology.
- 7.7. Computers attached to the LAN/WAN/Internet must meet currently adopted PCS security standards.

## **8. System Security**

- 8.1. Users shall protect the confidentiality of their password(s) to ensure system security and their own privilege and ability to continue to use the system.
- 8.2. Abuse or unauthorized use of passwords is prohibited.
- 8.3. Users who have knowledge of security problems or breaches of security by others are expected to notify a system administrator.
- 8.4. Any user identified as a security risk for having a history of problems with other computer systems may be denied access to computer facilities.

## **9. Internet Safety**

The PITTSYLVANIA COUNTY SCHOOLS shall prevent access to materials considered to be harmful to students as defined in Virginia Code Section 18.2-390 and 47 U.S.C. §254.(h)(7)(6). A filtering system will be used to prevent student access to materials containing pornography as set out in Virginia Code Section 18.2-374.1:1 and 18 U.S.C. §2256 and obscenity as defined in Virginia Code Section 18.2-372 and 18 U.S.C. §1460. Hardware and software systems have been implemented to prevent unauthorized online access, including "hacking" and other unlawful activities (reference *Internet Privacy Policy* KBE-PC).

- 9.1. PITTSYLVANIA COUNTY SCHOOLS employs spam filters and Internet content filtering by category in meeting federal and state guidelines for Internet safety. Users may encounter material which students, parents, teachers or administrators may consider to be obscene, inappropriate or offensive. Because of the global nature of the Internet, PITTSYLVANIA COUNTY SCHOOLS is not in a position to prevent all unsolicited or unintentional receipt of such materials. Students and staff are expected to refrain from sending, receiving, viewing, or downloading illegal material via the Internet.
- 9.2. PITTSYLVANIA COUNTY SCHOOLS provides filtered access to the Internet. Sites are categorized and restricted based on these categories. Sites not categorized are prohibited from student access until reviewed. Sites deemed to be inappropriate are placed in blocked categories. Security profiles are based on the physical address of the work station. Work stations are divided into two groups: staff and student. Student work stations have generic logins and staff work stations have personal IDs and passwords. Staff may override certain categories of sites and request evaluations of sites not categorized. The blocked categories are "pornography" and "gambling."

(continued)

- 9.3. PITTSYLVANIA COUNTY SCHOOLS blocks certain sites that contain images that may be pornographic in nature. In particular, child pornography and other obscene, vulgar, or educationally inappropriate materials are blocked.
- 9.4. The PITTSYLVANIA COUNTY SCHOOL BOARD is committed to complying with the Privacy Protection Act of 1976, Virginia Code Ann. §2.1-377 et seq., as defined in its Internet Privacy policy (KBE-PC). Before any image, article, or identifying information about a student is placed on a web site accessible from the public Internet, a release form must be signed by the parent/guardian.
- 9.5. This policy conforms to legislation approved by the 2006 General Assembly, Code §22.1-70.2 and with Superintendent's Memo 210, October 6, 2006, Guidelines and Resources for Internet Safety in Schools.
- 9.6. A matrix of roles and responsibilities of division personnel and community stakeholders will be included in this program's guidelines.

#### **10. Notification**

- 10.1. Effective with the 2007 – 2008 school year, the AUP and associated Student Conduct policies will be provided to each student and parent as part of the school handbook at the opening of school. Each student and parent/guardian must return a signed acknowledgement of their receipt of these policies.
- 10.2. AUP training will be conducted for students annually at the beginning of the school year by classroom teachers and/or Instructional Technology Resource Teachers.
- 10.3. AUP training will be conducted annually during pre-service workshops for all new employees. PCS employees will be notified of changes to the AUP on the division's home page and through information disseminated at the school level. School administrators will be notified of any changes during annual administrative workshops.
- 10.4. The division's COMPUTER TECHNOLOGY ACCEPTABLE USE AND INTERNET SAFETY POLICY will be posted on the division home page in standard electronic format.

ADOPTED: August 12, 1997

REVISED: August 10, 1999  
December 14, 1999  
August 14, 2001  
October 9, 2001  
May 8, 2007  
August 10, 2010

---

Legal Ref.: Code of Virginia, 1950, as amended, §§ 18.2-37, 18.2-374.1:1, 18.2-390, 22.1-70.2 and 22.1078, 18.2-374.1, 18.2-374.3, 18.2-376.1 and 18.2-152.7:1.

18 U.S.C. §§ 1460, 2256.  
47 U.S.C. § 254.