

GENERAL SCHOOL ADMINISTRATION

Computer Systems and Network Services - PWCS Acceptable Use and Internet Safety Policy

This regulation contains the Acceptable Use and Internet Safety Policy of the Prince William County Public Schools, as authorized in Policy 295, Standards for Use of Telecommunications and Internet Technologies. This governs the use of all Prince William County Public Schools (PWCS) local area networks, wired and wireless, wide area networks, the Internet/Intranet/Extranet-related systems, all PWCS Web sites, and all other similar networks. This policy also specifically applies to the use of PWCS computer equipment; software; operating systems; storage media; network accounts providing access to network services, such as email; Web browsing and file systems; as well as telecommunication technologies such as telephones, personal computers, cellular phones, Personal Digital Assistants (PDAs), facsimile machines, and all other wired or wireless telecommunication devices. To the extent this regulation can apply to other information and telecommunication technologies, it shall be interpreted to apply to them as well. This document supersedes all previous Acceptable Use policies and regulations for Prince William County Public Schools.

I. PWCS Instructional Philosophy

Prince William County Public Schools is committed to providing a World-Class education to meet the educational needs of our diverse student population. The instructional program in PWCS is implemented through a planned systematic approach which outlines the knowledge and skills to be taught in each subject and grade level.

Technology is a valuable tool that supports and enhances the PWCS instructional program by promoting problem solving, critical thinking, analytical, and decision making skills. Students and staff will access, process, and communicate information in a dynamic, integrated, and technological environment.

II. Expectation of Privacy

Employees and students have no expectation of privacy in their use of school computers or internet services, nor does the use of PWCS computers or related venues create an open or limited forum under the First Amendment to the federal or state constitutions. The Division retains the right to monitor all computer and Internet activity by employees and students, and any information or communications on PWCS computer systems and network services may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Use of PWCS computers, networks, and Internet systems is a privilege, not a right, and can be withdrawn by the Division at any time.

III. Acceptable Uses of PWCS Computer Systems and Network Services

It is the general policy that Prince William County Public Schools' computer systems and network services are provided for administrative, educational, communication, and research purposes consistent with the Division's educational mission, curriculum, and instructional goals. General rules and expectations for professional behavior and communication apply to use of the Division's computers, networks, and Internet services, as do those rules of student conduct set forth in the PWCS Code of Behavior. Acceptable uses of computer systems and network services include activities that support teaching and learning. Acceptable activities in support of this purpose include, but are not limited to, professional development, administrative communications, grant applications, new project announcements, and student product publishing.

A. Acceptable Use by Employees

Employees are to utilize the Division's computers, networks, and Internet services for school-related purposes and performance of job duties. Incidental personal use of school computers is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations, or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications not occurring during instructional time, which use is not otherwise prohibited by this regulation.

B. Unacceptable Uses of PWCS Computer Systems and Network Services

Any infraction of the regulation will not be tolerated and PWCS will act quickly in correcting the issue if the Acceptable Use and Internet Safety Regulation is not followed. Any user found to have violated this regulation, Regulation 295-2, Web Site Development and Implementation, any other applicable School Board policy or regulation, or applicable provisions of the PWCS Code of Behavior are subject to disciplinary measures, up to and including, revocation of privileges; student discipline, up to and including expulsion; administrative action; employee discipline, up to and including dismissal; and criminal prosecution under applicable local, state and/or federal law.

C. Examples of Unacceptable Uses of PWCS Computer Systems and Network Services

The following is a non-inclusive list of examples of unacceptable actions or activities:

1. Any use that is illegal or in violation of other School Board policies or regulations;

2. Violating the rights to privacy of any student or employee;
3. Transmitting, downloading, storing, or printing files or messages (text, sound, still, or moving graphics, or any combination thereof) that are pornographic, or are obscene, as defined at Va. Code §18.2-372, or that use language, sounds, or imagery which is lewd or patently offensive (including “sexually explicit visual materials” as defined at Virginia Code §18.2-374.1), or degrades others (the administration invokes its discretionary rights to determine suitability in particular circumstances);
4. Transmitting, downloading, storing, viewing, or printing files or messages (text, sound, still or moving graphics, or any combination thereof) that are plainly offensive, lewd, vulgar, or are otherwise inconsistent with the curricula and educational mission of PWCS;
5. Harassment by computer, which includes transmitting any material or posting material on any Web site which is threatening to another person, or which is intended to coerce, intimidate, or harass; material intended to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature; or material threatening any illegal or immoral act, whether or not such material is transmitted to that third person;
6. The School Division has no legal responsibility to regulate or review off-campus Internet messages, statements, postings, or acts. However, PWCS reserves the right to discipline students or employees for actions taken off-campus, which would violate this Regulation if occurring on-site, if such actions adversely affect the safety, well-being, or performance of students while in school, on school buses, at school activities, or coming to and from school; if such actions threaten violence against another student or employee, if such actions violate local, state or federal law, or School Board policies or regulations or the Code of Behavior, or if such actions disrupt the learning environment, administration, or orderly conduct of the school. The Division may also take appropriate disciplinary measures, up to and including dismissal, for off-campus Internet activities which are inconsistent with the professional and ethical standards expected of PWCS employees as “role models” for PWCS students.
7. Copying and/or installing proprietary information, including software, in violation of software licensing agreements and applicable law;

8. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music or videos, and the installation of any copyrighted software for which PWCS or the end user does not have an active license is strictly prohibited;
9. Using the PWCS network or information contained on the network for personal financial gain, commercial, advertising, solicitation or business activity not on behalf of the Prince William County Public Schools, unless authorized under Regulation 923-1, Commercial Advertising, or any illegal activity;
10. Any use for a forum for communicating by email or any other medium with other school users or outside parties to solicit, proselytize, advocate, or communicate the views of an individual or non-school-sponsored organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or non-profit. No employee shall knowingly provide names, email addresses, or other personal information to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable shall seek further guidance from their supervisor or the Director of Information Technology;
11. Sending mass emails to school users or outside parties for school or non-school purposes without the permission of an administrator;
12. Use of the PWCS network for political purposes, including any use requiring students to convey or deliver any materials that (a) advocate the election or defeat of any candidate for public office; (b) advocate the passage or defeat of any referendum question; or (c) advocate the passage or defeat of any matter pending before the School Board, the Prince William County Board of Supervisors, or the General Assembly of Virginia, or the Congress of the United States;
13. Any attempt to access unauthorized sites;
14. Any attempt to delete, erase or otherwise conceal any information stored on a school computer which violates these rules, or at any time after being advised by any administrator or supervisor to preserve any materials stored on a school computer;

15. Deliberately trying to degrade or disrupt system or network performance. Such acts will also be viewed as criminal activity under applicable state or federal law;
16. Transmitting or displaying messages promoting the sale of products/ services, except as provided in Regulation 923-1, Commercial Advertising.
17. Attempts to modify system facilities, downloading, installing, or transmitting viruses from email attachments or any other source, illegally obtaining extra resources, or attempting to subvert the restrictions associated with any computer system, computer account, network service, or personal computer protection software;
18. Writing down passwords and storing them anywhere accessible to others. Storing passwords in a file on ANY computer system (including PDAs or similar devices) without encryption;
19. Re-posting personal communications without the author's prior consent;
20. Transmitting unsolicited email messages or chain letters otherwise inconsistent with the curricula and educational mission of PWCS;
21. Personal use not related to educational or administrative purposes;
22. Fundraising or links to fundraising information on school/department Web sites or the Prince William County Public Schools Web page;
23. Sending PWCS proprietary and classified information to unauthorized persons, or posting this information outside of PWCS;
24. Distributing any school interior maps, floor plans, or written descriptions of interior floor plans on Web pages, camera locations, or other information which could compromise school security; and
25. Any content prohibited by Regulation 295-2, Web Site Development and Implementation.

IV. Areas of Responsibility

Employees, students, contractors, consultants, temporary employees of PWCS, including all personnel affiliated with third parties, volunteers in PWCS, and all other persons granted

access to the PWCS network infrastructure must comply with, and are responsible for monitoring, enforcing, and reporting infractions of the PWCS Acceptable Use Policy.

- Central Office Managers (i.e., department supervisor or director) and Principals and other school-based administrators shall be responsible for ensuring that this Acceptable Use Policy and Regulation 925-2, Web Site Development and Implementation, and Commercial Advertising are followed. Administrators shall also monitor teacher use and supervise correct integration of technology into instruction.
- Web Managers within schools and central office departments shall also be responsible for ensuring that this Acceptable Use Policy and Regulations 923-1, Commercial Advertising, and 925-2, Web Site Development and Implementation, are followed.
- Teachers shall be responsible for guiding and monitoring student use of PWCS computer systems and network services and for providing Internet safety instruction to students.
- Students shall be responsible for adhering to the PWCS Acceptable Use and Internet Safety Policy and regulation and using PWCS computer systems and network services for assignments directly related to the curriculum.
- Parents shall be responsible for ensuring that their children adhere to the PWCS Acceptable Use Policy and regulation and use PWCS computer systems and network services for curriculum related assignments.

V. Security

A. Technology Protection Measures.

To the extent practical, technology protection measures (or “Internet filters”) shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children’s Internet Protection Act [Pub. L. No. 106554 and 47 USC 254(h)], blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, and the approval of the Director of Information Technology Services or designee, technology protection measures may be disabled or, in the case of minors, minimized for a bona fide research or other lawful purposes. Prince William County Public Schools Information Technology Services has implemented and maintains industry leading technologies to secure and provide safe Internet access to students and staff. Internet filtering complements Prince William County Public Schools’ overall security strategy by use of a

holistic approach in protecting students, employees, and network assets. PWCS filters and monitors Internet activity through technology protective measures used to block or filter Internet or other forms of electronic communications. Filtering shall be applied to all materials deemed inappropriate, in accordance with applicable laws. Subject to staff supervision, technology protection measures may be bypassed, or in the case of minors, minimized, for bona fide research or other lawful purposes. Authority for bypassing or modifying any technology protection measure must be obtained from the Director of Information Technology Services or his/her designated representative. It shall be the responsibility of all Prince William County Public Schools staff to supervise and monitor usage of the computer network and access to the Internet in accordance with applicable federal and state laws, guidelines, and regulations of the Virginia Department of Education, and School Board policies and regulations.

B. Employee and Student Data Privacy

These standards are structured to provide due diligence and compliance with applicable federal, state, and local laws and School Board policies and regulations for the protection of confidential information and privacy of student and employee information during the collection, transfer, storage, use, disclosure, and destruction of such information. To protect the privacy of employees and students, school system personnel are legally responsible for safeguarding the information collected about and from employees and students. The data should be kept intact from accidents, unauthorized access, theft, unauthorized changes, or unintentional release. Data handlers should understand what is considered appropriate and inappropriate access to data and use thereof. Changes, alterations, and distribution of data must be made only in authorized and acceptable ways. No encryption solution or file-sharing program may be utilized unless authorized and approved by the Director of Information Technology Services or designee.

The collection, use, and dissemination of personally identifiable student or employee information shall be strictly limited to bona fide educational or administrative purposes. Photos and names of students and staff are allowed on PWCS Web sites for the purpose of publicizing school activities or student achievement, but such information must be used with caution and in accordance with Regulation 790-3, Release of Directory Information, which gives students and their parents/guardians the right to opt out of public disclosure of their names, photos, and other student information. Information regarding individual students may only be used if it meets the definition of directory information contained in Regulation 790-3, and the student/parent/guardian has not opted out of such disclosure.

Social security numbers shall not be collected, disseminated, or disclosed, unless authorized by law. Personal information, such as names, job titles and descriptions, telephone and fax numbers, email and other addresses, may be collected and used internally for PWCS program/ seminar registration via the Internet or for participation in PWCS online programs or other legitimate PWCS purposes. Such information shall not be sold or shared with any external groups nor disclosed to any third party outside PWCS.

Files containing confidential or sensitive data may not be stored on removable media or mobile devices taken off PWCS property unless approved by the central office department manager /school principal and protected by an approved Information Technology Services encryption solution.

Individuals or companies under contract with PWCS may have access to information in the course of the service they provide to PWCS, but those entities are not permitted to use or re-disclose that information for unauthorized purposes and must sign a PWCS nondisclosure agreement prior to work being performed. No other entities are authorized to collect information through PWCS sites.

Risk Management must be notified immediately if sensitive or critical PWCS information is compromised or lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of PWCS information systems has taken place, or is suspected of taking place.

C. Access to PWCS Computer Systems and Network Services

Employees, students, and temporary employees of PWCS acknowledge their understanding of the Acceptable Use and Internet Safety Policy as a condition of receiving access to the computer system and network services. All employees will be reminded of the PWCS Acceptable Use expectations annually in employee newsletters (i.e. “Communicator,” “the Leader”). Building administrators and/or department supervisors are responsible for reviewing the expectations with their staff.

D. User Accounts

All user-level, system-level, email, and application services must have a unique user identification. Users shall not allow others access to their account and are responsible for all activities performed with their account. Additionally, employee and students must not use the accounts of others to perform activities on PWCS information resources. It is the user’s responsibility to ensure that this identification is not shared with others. Quarterly review of user accounts will be performed to purge outdated user accounts and to ensure compliance with this regulation.

- Use of generic and temporary network, application, and email accounts should not be deployed, unless approved by the Director of Information Technology Services or designated representatives.
- Users are not allowed more than one concurrent session and restricted access to PWCS business hours, unless authorized by the Director of Information Technology Services or designee.

- Employees are required to log out of computer sessions daily and prior to allowing another user access to a computer system in which they have an active session. Employees shall be responsible for any unauthorized use of a computer, network, or Internet system by any person or student who accesses the same because or while the employee has failed to log out as required.
- Laptop users are required to first login to the PWCS network via their network login account to create a local user account on the laptop system in order to provide logging and accountability of use while off site.

E. Authentication

Authentication is a method used to validate a user's authorization to access to a computer system or application. Users shall adhere to the following authentication procedures:

- Administrator and employee computer systems shall employ a PWCS-approved screen saver with "on resume password enable" required after 10 minutes.
- Users shall secure computer systems via the password protected screen saver when leaving computer systems unattended. This feature prevents unauthorized use of a computer system after a legitimate user has logged on, but is momentarily away from their computer. Public and student computers, such as those in the library or in labs, with no critical or sensitive information are excluded.
- Session time-outs of no more than five minutes are required on Web-based applications.
- Network connected computer systems and Web application services owned by PWCS shall have a warning banner on all access points and ensure that the banner is displayed whenever the system is turned on or at user login.

F. Passwords

A password is used in conjunction with a unique user identification in order to authenticate a user's right to access a computer system and application service. Passwords help protect against misuse by seeking to restrict use of PWCS systems and networks to authorized users. Authorized users are responsible for the security of their passwords and accounts. Passwords are considered secret and are not to be shared under any circumstance. Individual user passwords must never be embedded into an application or process. All user-level, system-level, email, and application service passwords must conform to these guidelines. Public computers, such as those in a library or in labs, with no critical or sensitive information, may be excluded on

a case-by-case basis, as approved by the Director of Information Technology Services or designated representatives.

A password should be assigned to each unique user identification. Users are required to change passwords immediately upon first logging into the system and/or application.

If an account or password is known or suspected to have been lost, stolen, or disclosed, the user shall immediately report the incident to the Director of Information Technology Services or designated representatives, and change all passwords. Password requirements are located in Appendix III.

G. Email Accounts

Employees are assigned PWCS email accounts, to be utilized for educational purposes and official PWCS Division communication. Automated forwarding of email messages should be disabled unless authorized by the Director of Information Technology Services or designated representatives to prevent proprietary and classified information leaking to unauthorized persons or entities.

If students are assigned email accounts, a teacher must act as a sponsor. Sponsors are responsible for guiding and monitoring student communication and use of appropriate sections of the network and for assuring that students understand that misuse of the network will cause them to lose their accounts and/or face disciplinary action. When appropriate, sponsors will assume responsibility for teaching the students proper techniques and standards for participation; explain issues of privacy, copyright infringement, tool use, and network etiquette.

H. Hardware and Software

Software utilized by schools or individual departments that is intended for use on the PWCS network must be reviewed by the Information Technology Steering Committee prior to purchase or installation and approved by the Director of Information Technology Services or designee. The Department of Information Technology Services is responsible for obtaining and verifying the proper written authorization from information asset owners for granting access to system and/or application resources implemented on network connected computer systems. End users cannot install, run, or download software or modify configurations on network connected computer systems unless authorized by Information Technology Services. This stipulation is to ensure compliance with copyright laws, patch management, malware avoidance and overall infrastructure and computer system integrity. Installation of network connected computers, maintenance, repair, updates including hardware, and software, should be approved, directed, and completed by Information Technology Services.

The Division's malware/anti-virus software must be installed, enabled, and kept up-to-date on all network connected computer systems at all times. The malware/anti-virus software should be managed centrally and not configurable by end users. Weekly system scans should be performed on all computer systems. Malware infected computer systems must immediately be remediated or removed from the network until they are verified as malware-free.

As new vulnerabilities are discovered and software upgrades become available, computer systems must have the most recently available and appropriate software security patches, commensurate with the identified level of acceptable risk.

All systems (e.g., computers, monitors, printers) should be turned off at the end of the school/work day and on days when schools/offices are closed, with the exception of days/times established to allow for after-hours malware/anti-virus system scans and software/operating systems patch maintenance/upgrades (e.g., leaving computers on every Wednesday and Thursday evening). On occasion, schools/offices may be directed to leave computers on for special reasons/urgent matters concerning updates or data security issues that must be attended to immediately.

I. Remote Access

It is the responsibility of PWCS employees, contractors, vendors, and agents with remote access privileges to the PWCS network to ensure that their remote access connection is given the same consideration as the user's on-site connection to PWCS. All users in need of remote access to PWCS assets are required to use centrally administered tools and comply with the Information Technology Services Firewall Standards. Organizations or individuals who wish to implement non-standard remote access solutions to the PWCS network must obtain prior approval from the Director of Information Technology Services or designee. All computer systems that are connected to the PWCS internal network via remote access technologies must comply with all requirements of this regulation.

VI. Incident Response, Mitigation, Management, and Investigation

Incident response seeks to facilitate the discovery, management, mitigation, investigation, and awareness of computer system and network service related security incidents in a manner that complies with applicable laws, policies, and regulations. All identified security related incidences shall be reported to a site administrator or PWCS Risk Management Department immediately. PWCS Risk Management Department or the Director of Information Technology Services or designated representatives shall verify that an incident has occurred and determine what, if any, action needs to be taken (Appendix III). No user shall power off/on, disconnect, delete information from, or otherwise disturb any computer subject to seizure, unless under the direction of Risk Management or the Director of Information Technology Services or designated representatives.

VII. Preservation of Electronic Evidence

When the Division has notice of actual or anticipated litigation, it is required to preserve all evidence, including electronic evidence, related to such litigation. Employees who receive notice from PWCS of actual or threatened litigation (or become aware of such actual or threatened litigation from other sources) must preserve all such evidence and may not delete, alter, or otherwise disturb the integrity of any electronic evidence. This includes, but is not limited to, emails, files, folders, or any other electronic data or communications.

VIII. Internet Safety Instruction

Internet safety instruction is the responsibility of all instructional personnel. “NetSmartz”, K-12 Internet safety curriculum provided by National Center for Missing & Exploited Children, and additional resources will be used with students at all grade levels.

The Internet Safety instructional plan can be found in Appendix III.

IX. Review Process

The Associate Superintendent for Communications and Technology Services (or designee) is responsible for implementing and monitoring this regulation and the Acceptable Use Policy.

The Associate Superintendent for Communications and Technology Services (or designee) is responsible for reviewing this regulation and the Acceptable Use Policy annually, with the assistance of the PWCS Department of Information Technology Services and Office of Instructional Technology. Every two years, the Division Superintendent will file an Acceptable Use Policy with the state that has been approved by the PWCS School Board.

APPENDIX I:

Resources

Contacts for Security Incidents

- Site administrator, principal, guidance counselor, or department supervisor
- Risk Management and Security Services 703.791.7206
- Department of Information Technology Services 703.791.8722

Prince William County Public Schools Code of Behavior

<http://pwcs.edu/student-services/codeofbehavior.pdf>

APPENDIX II

Password Requirements

- Minimum characters: 8
- Passwords must contain at least one letter, one numeral, and one special character
- No repeatable/consecutive characters
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain numeric/special characters, such as 0-9, !@#\$%^&*()
- Password should not contain a word found in the (English) dictionary
- Expiration settings – at least once every six months
- None of a user's previous 3 passwords can be re-used
- Accounts should automatically lock after 3 consecutive failed login attempts for at least 30 minutes to sufficiently stop brute force password hacks with strong passwords enabled

APPENDIX III:

Internet Safety Instructional Plan

Schedule of Implementation

April, 2007	Research and develop Internet Safety program and implementation plan.
May, 2007	Review "NetSmartz" curriculum
Sept. - Dec., 2007	Determine concepts that will be taught at specific grade levels and develop any additional resources that are needed. Develop an online course to be accessed by teachers and administrators
Dec., 2007	Professional Development for Instructional Technology Resource Teachers Select schools to pilot curriculum
Jan. - Feb., 2008	Provide face to face and online professional development for teachers that will pilot the curriculum
Feb. - Apr., 2008	Pilot curriculum at selected schools
May - June, 2008	Evaluate pilot program
Aug., 2008	Report pilot results to Virginia DOE
Sept., 2008	Submit report to Virginia DOE with revised AUP and Internet Safety program. Full implementation of Internet Safety program

Professional Development

Summer, 2007	Acceptable Use Regulation training for administrative staff
Sept., 2007	Site-based Acceptable Use Regulation training for school staff
Yearly in Sept.	Annual review of AUP by all PWCS staff
Dec., 2007	Professional development for Instructional Technology Resource Teachers
Jan. - Feb., 2008	Face to face and online professional development for schools that will pilot the Internet Safety curriculum
Spring, 2008	Face to face and online professional development for all schools

Community Outreach and Training

- Internet Safety presentation at annual Technology Showcase
- School-based parent and community meetings
- Collaboration with PWC Police Department and School Resource Officers to develop Internet safety protocols and curriculum
- Use of available public communications (PWCS television network) to provide Internet safety information to parents and the community