Bring Your Own Device: Pennington Public Wi-Fi

Guidelines at a Glance

PWCS is now offering a filtered PWCS Public Wi-Fi on all campuses. Pennington students may bring a personal device to school and use for educational purposes. Students are expected to connect to the filtered PWCS Public-WiFi to ensure access to the best online resources. We recommend that you clearly label all devices and power cords with your student’s name and set password or passcode on the device.

Important Facts

- Pennington students may now bring their own technology devices (laptop, netbook, cell phone, tablet, etc.) to school where they will be utilized in the classroom at the discretion of the teacher.
- Students are expected to connect to the PWCS Public Wi-Fi, and adhere to the terms of the PWCS Acceptable Use Policy (AUP) as well as the Pennington Responsible Use Guidelines (RUG), located on the Pennington Website.
- Use of technology is a privilege and not a right.

Responsibility for Devices

- The technology devices students bring to school are their sole responsibility.
- The school or county assumes no responsibility for personal devices if they are lost, loaned, damaged, or stolen and only limited time or resources will be spent trying to locate stolen or lost items.
- Personal devices may be subject to investigation in accordance with County Policy.
- Students are to keep their devices secure at all times and not loan to others.
- Students must keep devices on silent or vibrate mode.
- Each student is responsible for his/her own device: set-up, maintenance, and charging. Teachers will not store student devices at any time, nor will any County employee diagnose, repair, or work on a student’s personal device.
- Photos and videos are only to be taken when directed by the classroom teacher.

<table>
<thead>
<tr>
<th>Location</th>
<th>Laptop, Netbook, Tablet, IPad</th>
<th>Cell Phone</th>
<th>iPod, Nintendo DS</th>
<th>eReader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classroom</td>
<td>As directed by teacher</td>
<td>As directed by teacher</td>
<td>As directed by teacher</td>
<td>As directed by teacher</td>
</tr>
<tr>
<td>Hallways, Bathrooms</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Library</td>
<td>As directed by librarian</td>
<td>As directed by librarian</td>
<td>As directed by librarian</td>
<td>As directed by librarian</td>
</tr>
<tr>
<td>Dining Area</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Note: When not in use, students are responsible for the safe keeping of their own device. Student may use their device before school prior to the first bell.
Pennington Traditional School
Student Responsible Use Guidelines for Technology (RUG)

Pennington makes a variety of communications and information technologies available to students through computer/network/Internet access. These technologies, when properly used, promote educational excellence in PWCS by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming its students and its employees. These Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating PWCS students and setting standards which will serve to protect PWCS. Pennington firmly believes that digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

Mandatory Review. To educate students on proper computer/network/Internet use and conduct, students are required to review these guidelines at the beginning of each school year. All Pennington students shall be required to acknowledge receipt and understanding of all guidelines governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such guidelines. The parent or legal guardian of a student user is required to acknowledge receipt and understanding of Pennington’s Student Responsible Use Guidelines for Technology (hereinafter referred to as the Responsible Use Guidelines) as part of the Pennington’s Principal’s Guidelines and the Student Code of Behavior.

Definition of PWCS Technology System. The PWCS’s computer systems and networks (system) are any configuration of hardware and software. The system includes but is not limited to the following:
- Telephones, cellular telephones, and voicemail technologies;
- Email accounts;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, and video and audio files;
- Internally or externally accessed databases, applications, or provided Internet access;
- PWCS-filtered public Wi-Fi; and
- New technologies as they become available.

Availability of Access
Acceptable Use. Computer/network/Internet access will be used to enhance learning consistent with the PWCS’s educational goals. PWCS requires legal, ethical and appropriate computer/network/Internet use.

Privilege. Access to the PWCS’s computer/network/Internet is a privilege, not a right.

Access to Computer/Network/Internet. Access to the PWCS’s electronic communications system, including the Internet, shall be made available to students for instructional purposes. Computers, whether wireless or wired, has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children’s Internet Protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA.

Student Access. Computer/network/Internet access is provided to all students. Student Internet access will be under the direction and guidance of a PWCS staff member. Students may also be allowed to use the local network and public Wi-Fi.

Use of Personal Electronic Devices. PWCS believes technology is a powerful tool that enhances learning and enables students to access a vast amount of academic resources. Our goal at Pennington is to increase student access to digital tools and facilitate immediate access to technology-based information, much the way that students utilize pen and paper. To this end, PWCS has opened a filtered, wireless network through which students in specific age groups will be able to connect privately owned (personal) electronic devices. Students using personal electronic devices must follow the guidelines stated in this document while on school property or while attending any school-sponsored activity.

Middle School – Students are allowed to bring personal electronic devices that can access the Internet for educational purposes as determined by the classroom teacher. Students will not be allowed to use the devices during passing periods or in the cafeteria setting.

Elementary – Students are allowed to bring personal electronic devices for academic classroom use as determined by the classroom teacher. Students will not be allowed to use the devices during passing periods or in the cafeteria setting.

Security - A student who gains access to any inappropriate or harmful material is expected to discontinue the access and to report the incident a staff member. Any student identified as a security risk or as having violated the Acceptable Use Policy (AUP) and/or Responsible Use Guidelines (RUG) may be denied access to the PWCS system. Other consequences may also be assigned. A student who knowingly brings prohibited materials into the school’s electronic environment will be subject to suspension of access and/or revocation of privileges on the PWCS system and will be subject to disciplinary action in accordance with the Pennington’s Principal’s Guidelines and the Student Code of Behavior.

Subject to Monitoring. All PWCS computer/network/Internet usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. Students should not use the computer system to send, receive or store any information, including email messages, that they consider personal or confidential and wish to keep private. All electronic files, including email messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. Pennington reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Students should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of Pennington. Personal electronic devices are subject to examination in accordance with disciplinary guidelines if there is reason to believe that the Responsible Use Guidelines have been violated.

School Based Technology Team & BYODITRT & TSSPEC Role:

The Instructional Technology Resource Teacher and Technical Support Specialist at each school will not work on personal devices brought to school by any PWCS staff (teachers, administrators, etc), or students. The function of the ITRT and TSSPEC with BYOD is to identify that the “Guest Wireless Network” is up and running. If PWCS staff and students still cannot connect to the PWCS “Guest Wireless Network”, than it is the responsibility of the
owner to troubleshoot the issue on their device. Students will not be held accountable during class if their device cannot connect. The teacher will have other avenues to ensure instruction is not impeded for the student.

Student Computer/Network/Internet Responsibilities
PWCS students are bound by all portions of the Responsible Use Guidelines. A student who knowingly violates any portion of the Responsible Use Guidelines will be subject to suspension of access and/or revocation of privileges on the PWCS’s system and will be subject to disciplinary action in accordance with the Pennington’s Principal’s Guidelines.

Use of Social Networking/Digital Tools. Students may participate in PWCS-approved social media learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and on-line meeting sessions. The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other PWCS-approved digital tools.

Password Confidentiality. If a student’s device is password protected they are required to maintain password confidentiality by not sharing their password with others. Students may not use another person’s device.

Reporting Security Problem. If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the student should immediately notify the supervising staff member. The security problem should not be shared with others.

The following guidelines must be adhered to by students using a personally-owned electronic device at school:

- Internet access is filtered by PWCS personal electronic devices in the same manner as PWCS-owned equipment. If network access is needed, connection to the filtered, wireless network provided by PWCS is required.
- These devices are the sole responsibility of the student owner. Pennington assumes no responsibility for personal electronic devices if they are lost, loaned, damaged or stolen and only limited time or resources will be spent trying to locate stolen or lost items.
- These devices have educational and monetary value. Students are prohibited from trading or selling these items to other students on PWCS property, including school buses.
- Each student is responsible for his/her own device: set-up, maintenance, charging, and security. Staff members will not store student devices at any time, nor will any PWCS staff diagnose, repair, or work on a student’s personal electronic device.
- Electronic devices are only to be used for educational purposes at the direction of a classroom teacher or as stated for specific age groups.
- Administrators and staff members have the right to prohibit use of devices at certain times or during designated
- Staff and administrators may examine a student’s personal electronic device and search its contents, in accordance with disciplinary guidelines.

Inappropriate Use
Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/network/Internet system or any components that are connected to it. The following actions are considered inappropriate uses, are prohibited, and will result in revocation of the student’s access to the computer/network/Internet.

Violations of Law. Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:
- threatening, harassing, defamatory or obscene material;
- copyrighted material;
- plagiarized material;
- material protected by trade secret; or
- blog posts, Web posts, or discussion forum/replies posted to the Internet which violate federal or state law.

Transmitting Confidential Information. Students may not redistribute or forward confidential information without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing personal information about oneself such as, but not limited to, home addresses, phone numbers, email addresses, birthdates or of others is prohibited.

Plagiarism. Fraudulently altering or copying documents or files authored by another individual is prohibited.

Inappropriate Language. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in emails blogs, wikis, or other communication tools is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.

Consequences of Agreement Violation
Any attempt to violate the Pennington’s Principal’s Guidelines may result in revocation of the student’s access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary and/or appropriate legal action may be taken.

Denial, Revocation, or Suspension of Access Privileges. With just cause, the System Administrator and/or building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

Warning
Sites accessible via the computer/network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each PWCS computer with Internet access has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children’s Internet Protection Act. PWC makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Electronic Devices:
- Teachers have the control of when and what type of electronic devices will be used in the classroom.
- As with reading a printed book, students reading from eReaders should be permitted to read as you would with a printed book.
- Students should not be sitting in the hallway using their devices.
- All personal devices used in the classroom are for class activities to access the Internet or other capabilities as deemed appropriate by the teacher.
Guidelines for Use of Personal Telecommunication Devices

Learning about and being held accountable for the responsible use of either county-owned technology or personally owned electronic devices is an important part of preparing students to be successful in the future. Whether using county or personally-owned electronic devices for school purposes, each student is expected to act in an appropriate manner in accordance with the Responsible Use Guidelines (RUG).

---

Guidelines for Use of Personal Electronic Devices

I have read, understand, and will abide by all the guidelines set forth above regarding the use of personal electronic devices at Pennington Traditional School. I understand that violations of these guidelines may result in the loss of county network and/or computer privileges either temporarily or permanently, as well as any other disciplinary action in accordance with the student code of conduct. I understand that this document and the Pennington Responsibility Use Guidelines, supersedes the Code of Conduct in that the level II infraction on usage of electronics will be interpreted as misuse of electronics.

<table>
<thead>
<tr>
<th>Signature of Student</th>
<th>Printed Name of Student</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I have reviewed and discussed this document with my child. My child understands the expectations and responsibilities associated with the proper care and handling of personal electronic devices while at school. My child is clear that the consequences of not upholding his/her responsibilities may result in disciplinary actions in accordance with the student code of conduct.

<table>
<thead>
<tr>
<th>Signature of Parent</th>
<th>Printed Name of Parent/Guardian</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>