PULASKI ACADEMY & CENTRAL SCHOOL
STAFF AND STUDENT NETWORK ACCEPTABLE USE POLICY

Please review this entire Acceptable Use Policy carefully before you sign it and return it with your child. It will give both you and your student a clear understanding of how our school's computer network is intended to be used. By adhering to this policy, we can ensure that both Pulaski Academy's network and the Internet are used to their fullest educational potential.

Filtering

Under the Children's Internet Protection Act, which was passed by Congress and signed by President Clinton in December, 2000, all schools which receive an "E-Rate" discount on their internet service are required to meet certain provisions for all computers that have Internet access.

Since September of 1999, Pulaski Academy has had in place filtering software – commonly called a "firewall" – to help guard our students against inappropriate or harmful information. The firewall is configured to block access to inappropriate internet websites. The block is in operation 24 hours a day, 7 days a week, and applies to both students and staff/faculty. Our software is provided by the Sonic Corporation, whose role it is to research websites and determine if the content falls into one of the configured categories. The filter list is automatically updated and downloaded to our firewall. In addition, we are able to add specific domains to the "forbidden" list, and enter keywords to stop searches in particular areas.

Also, we try to limit access to websites that are not educationally based or appropriate for school use, such as games, instant messaging, social networking, and chat services, even though they may not be considered particularly "harmful." In spite of the constant monitoring and updating, it is impossible for the firewall to find and block every harmful website – there are literally millions of them out there.

Monitoring and Education

To keep our students safe, we will also continue to monitor student utilization of the district computers and the Internet, and provide age appropriate online behavior and internet safety education to our students. This education includes safely interacting with other individuals on social networking sites and in chat rooms, as well as cyberbullying awareness and response while utilizing internet resources.

Mobile Devices

Pulaski Academy recognizes that the use of mobile devices in schools are now an integral part of our students' culture and way of life, and can have considerable value, especially playing a significant part in the education of the 21st century student. We further recognizes that the use of mobile devices in schools presents a host of potential problems and disadvantages. The term "mobile device", as used in this policy, covers smart phones, laptop computers, tablet devices such as the iPad or Android devices, e-readers such as Kindle or Nooks, iPod touch devices or any similar mobile electronic device that can access the Pulaski Academy wireless network.

The use of mobile devices at Pulaski Academy is a **privilege** and **not a right**. Any and all network equipment, and all computerized files and data accessed through the Pulaski network are the property of Pulaski Academy. Consequently, no user of the Pulaski Academy wireless or wired network should have any expectation of privacy with respect to any files or data saved on or accessed through the Pulaski network.

The district assumes no liability or responsibility for students that misuse mobile devices while on school property, as well as accepts no financial responsibility for damage, loss or theft of personally owned devices. The use of mobile devices on the district's wireless network should be limited to educational purposes. Any use of a mobile devices that interferes with or disrupts the normal procedures of the network or educational environment is prohibited.

Administration

1. The Superintendent of Schools shall designate a Technology Director to oversee the district's computer network.
2. The Director and his/her designee shall monitor and examine all network activities as deemed appropriate to ensure proper use of the system.
3. He/She shall disseminate and interpret district policy and regulations governing use of the district's network at the building level with all network users.
4. He/She shall provide employee training for proper use of the network and will ensure that staff supervising students using the district's network provide similar training to their students, including copies of district policy and regulations governing use of the district's network.
5. He/She shall ensure that all computers are properly guarded against possible virus/malware/trojan infections by keeping licensed virus protection software installed and up to date.
6. All staff and student agreements to abide by district policy and regulations shall be kept on file in the appropriate building.

System Access

The following individuals may be designated as members with access to the computer network system:

1. Elementary and secondary students may be granted an account for up to one academic year at a time.
2. Teachers and instructional staff members will have individual accounts.
3. Other district employees as deemed necessary.
4. Community members as deemed necessary.

Procedures for Proper Use

1. The district's physical and wireless computers and networks shall be used **only** for educational purposes consistent with the district's mission and goals.
2. Network users will be issued a log-in name and password.
3. The individual in whose name an account is issued is responsible at all times for its proper use.
4. This Acceptable Use Policy and all provisions contained also applies to students during school trips, excursions, camps and extra-curricular activities.
5. Network users identifying a security problem on the district's system must notify the appropriate teacher, administrator or computer coordinator. Do not demonstrate the problem to anyone.
6. Student account information will be maintained in accordance with applicable education records laws, and district policy and regulation 5500.
7. Copyrighted material may not be placed on any computer connected to the district's network without the author's permission. Only staff specifically authorized may upload copyrighted material to the network.
8. Faculty/staff network users may download copyrighted material for their own use. Copyrighted material shall be used in accordance with the fair use doctrine and district policy and regulation 8650.
9. Only district-owned instructional materials approved by the District Technology Director or the District Technology Committee may be loaded on the District network and machines.
10. Only staff members of the Technology Department may install software on individual machines.
11. Any network user identified as a security risk, or having a history of violations of district computer use guidelines, may be denied access to the district's network.

Privacy Rights

Users' data files and electronic storage areas shall remain District property, subject to District control and inspection. **This includes all archived data and email communications**. The Technology Director may inspect a file that contains data that violates district rules, policy or the law, and access all files and communications to ensure system integrity, and that users are complying with requirements of this policy and accompanying regulations**. Users should *NOT* expect that information accessed or stored on the Pulaski Academy network or domain will be private.** Electronic mail and telecommunications are not to be utilized to share confidential information about students or other employees.

Prohibitions

The following is a list of prohibited actions concerning use of the district's computer network. Violation of any of these prohibitions may result in discipline or other appropriate penalty, including detention, suspension or revocation of a user's access to the network.

- **Non-educational use of social networking, *all* instant messaging, blog sites and chat services are prohibited.**
- **Use of computer access to data other than for educational purposes is prohibited.**
- **Users will not attempt to gain unauthorized access to the network, or go beyond their authorized access.** This includes attempting to log on through another person's account or access another person's files, attempting to obtain passwords, or attempting to remove any existing network security functions. Users will not actively search for security problems, because this will be construed as an illegal attempt to gain access.
- **There must be no sharing of passwords. Attempts to log on to the district's system in the name of another individual, with or without the individual's password, is prohibited.**
- Users must not intentionally develop or use programs to harass other users, or attempt to violate the security or alter software components of any other network, service or system. Examples of such activities include hacking, cracking into, monitoring or using systems without authorization, scanning ports, conducting denial-of-service attacks and distributing viruses or other harmful software.
- Users must not attempt to damage hardware, software or data belonging to the school or other users. This includes adding, altering or deleting files or programs on local or network hard drives and removing or damaging any equipment such as mice, motherboards, speakers, or printers.
- Attempts to read, delete, copy or modify the electronic mail of other system users is prohibited as is deliberate interference with the ability of their system users to send/ receive electronic mail. Forgery or attempted forgery of electronic mail messages is prohibited.
- No personal software or disks may be loaded onto the district's computers and/or network.
- System users shall not encourage the use of tobacco, alcohol or controlled substances or otherwise promote any other activity prohibited by district policy, state or federal law.

PULASKI ACADEMY & CENTRAL SCHOOL - STAFF AND STUDENT NETWORK ACCEPTABLE USE POLICY, CONT'D

- Transmission of material, information or software in violation of any district policy or regulation, local, state or federal law or regulation is prohibited.
- **Downloading any file from the internet without a specific educational purpose, including program or executable application files, is prohibited.** Examples include, but are not limited to: wallpaper, screensavers, audio/video clips, inappropriate graphic files or images, and messenger services.
- Tampering with, misuse of, or vandalizing any component of the computer system or taking any other action inconsistent with this policy and regulation will be viewed as a security violation.

Consequences

The school may at its sole discretion determine whether a use of the network or a device is a violation of this policy. Violations of this policy may result in a demand for immediate removal of offending material, blocked access, suspension or termination of the users account, or other action appropriate to the violation. The school reserves the right to act without notice when necessary, as determined by the administration. The school may involve, and will cooperate with, law enforcement officials if criminal activity is suspected. Violators may also be subject to civil or criminal liability under applicable law. **Students who lose their network computer privileges are responsible for making arrangements with their teacher(s) for fulfilling class requirements.**

Any Middle/High school student found to be in violation of this agreement will face the following consequences:

1. **An attempt to gain unauthorized access to the network, or go beyond their authorized access** – privileges immediately revoked for the remainder of the school year, and 1 in school suspension
2. First offense of any other type – 1 Tuesday/Thursday detention
3. Second offense - 1 Saturday detention
4. Third offense - 1 in school suspension

Any offense may result in the removal or limitation of computer privileges.

Any Academic Center or Elementary school student found to be in violation of this agreement will face the following consequences:

1. **An attempt to gain unauthorized access to the network, or go beyond their authorized access** – privileges immediately revoked for the remainder of the school year, and 1 in school suspension
2. First offense of any other type – computer access privileges revoked for 2 days
3. Second offense - computer access privileges revoked for 1 week
4. Third offense - computer access privileges suspended for 1 semester.

Any Elementary student found in violation may result in parent/guardian contact before privileges are re-instated.

Any Staff member found to be in violation of this agreement will be handled by the Superintendent of Schools.

PLEASE RETURN THE FOLLOWING PORTION TO THE TECHNOLOGY OFFICE:

****

We have read this Acceptable Use Policy, understand its terms, and agree to abide by the agreement.

PLEASE PRINT STUDENT NAME CLEARLY: ____

_________________________________/____/___ _________________________________/____/___

Student Signature Date Parent Signature Date

User ID: ___________________ [User ID consists of the first initial, and the last name]

User Password: ___________________ **Each student chooses his/her own password.**

It must be a minimum of 5 characters – letters or numbers. PLEASE PRINT THE PASSWORD CLEARLY.