Acceptable Use Policy

These guidelines are provided so that students and parents are aware of the responsibilities students accept when they use District-owned hardware, operating system software, application software, stored text, data files, electronic mail, local databases, digitized information, communication technologies, and Internet access. In general, this requires efficient, ethical, and legal utilization of all technology resources.

- Expectations
  - Student use of computers, other technology hardware, software, and computer networks, including the Internet is only allowed when supervised or granted permission by a staff member.
  - All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center (library) of each campus.
  - Although the District has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening or make them feel uncomfortable.
  - Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.
- Unacceptable conduct includes, but is not limited to the following:
  - Using the network for illegal activities, including copyright, license, or contract violations or downloading inappropriate materials, viruses, and/or software, such as but not limited to hacking and host file sharing software.
  - Using the network for financial or commercial gain, advertising, or political lobbying.
  - Accessing or exploring online locations or materials that do not support curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.
  - Vandalizing and/or tampering with equipment, programs, files, software, system performance, or other components of the network. Bypassing internet filtering is strictly prohibited as is use or possession of hacking software.
  - Causing congestion on the network or interfering with the work of others, e.g. chain letters or broadcast messages to lists or individuals.
  - Intentionally wasting finite resources, i.e., online time, real-time music.
  - Gaining unauthorized access anywhere on the network. Revealing the home address or phone number of one's self or another person.
  - Invading the privacy of other individuals. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.
  - Coaching, helping, observing, or joining any unauthorized activity on the network.
  - Forwarding/distributing email messages without permission from the author.
  - Posting anonymous messages or unlawful information on the system.
  - Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, demanding, stalking, or slanderous.
  - Falsifying permission, authorization, or identification documents.

    - Obtain copies of or modify files, data, or passwords belonging to other users on the network. Knowingly placing a computer virus on a computer or network.
- Acceptable Use Guidelines — School District Network Resources and Services
    - General Guidelines – Students will have access to all available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.
    - Students are responsible for their ethical and educational use of the computer online services in the District.
    - All policies and restrictions of the District network services must be followed.
    - Access to the School District network services is a privilege and not a right. Each student, and/or parent will be required to sign the Acceptable Use Policy Agreement and adhere to the Acceptable Use Guidelines in order to be granted access to the District Network computer online services. The use of any network service in the District must be in support of education and research and in support of the educational goals and objectives of the District.
    - When placing, removing, or restricting access to specific databases or other District computer services, school officials will apply the same criteria of educational suitability used for other education resources. Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to: confidential information, copyrighted material, threatening or obscene material, and computer viruses.
    - Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual, campus administrator, or technology administrator will be considered an act of vandalism and subject to disciplinary action.
- Any parent wishing to restrict their children's access to any District computer online services will provide this restriction request in writing. Parents will assume responsibility for imposing restrictions only on their own children.
- Network Etiquette
    - Be polite.
    - Use appropriate language.
    - Do not reveal personal data (home address, phone number, phone numbers of other people).
    - Remember that other users of the PISD network services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

Consequences
The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use.

Non-compliance with the guidelines published here may result in suspension or termination of technology privileges and disciplinary actions. Use or possession of hacking software is strictly prohibited and violators will be subject to the Student Code of Conduct. Violations of applicable state and federal law will result in criminal prosecution, as well as disciplinary actions by the District. Electronic mail, network usage, and all stored files will not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use. The District cooperates fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws.