PRINCETON

INDEPENDENT SCHOOL DISTRICT

ACCEPTABLE USE OF COMPUTERS AND NETWORK RESOURCES

Handbook

PRINCETON ISD
ACCEPTABLE USE OF COMPUTERS AND NETWORK RESOURCES

It is the belief of the Princeton ISD Board of Education that the use of technology is an important part of preparing children to live in the 21st century. The Board further believes that a “technology rich” classroom can significantly enhance both the teaching and learning process. This technology includes PISD computer hardware, software, local and wide area networks, and internet access, as well as student owned digital devices voluntarily brought to school. Due to the complex nature of these systems and the magnitude of information available via the Internet, the Princeton ISD Board of Education believes guidelines regarding acceptable use are warranted in order to serve the educational needs of students.

It shall be the policy of the Princeton ISD Board of Education that the school system shall have in continuous operation, with respect to any computers belonging to the school having access to the Internet:

1. A qualifying “technology protection measure,” as that term is defined in Section 1703(b)(1) of the Children’s Internet Protection Act of 2000; and
2. Procedures or guidelines which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are (i) obscene, (ii) child pornography, or (iii) harmful to minors, as those terms are defined in Section 1703(b)(1) and (2) of the Children’s Internet Protection Act of 2000.

The district’s technology resources are provided for educational purposes that promote and are consistent with the instructional goals of the Princeton ISD School System. Use of computers and network resources outside the scope of this educational purpose is strictly prohibited. Students and employees accessing network services or any school computer shall comply with the district’s acceptable use guidelines. The Princeton ISD Employee Handbook contains expectations for teachers regarding *Use of PISD Technology Resources, Personal Use of Electronic Media,* and *Use of Technology Media with Students*.

The district reserves the right to monitor, access, and disclose the contents of any user’s files, activities, or communications. Princeton ISD also supports the *Bring Your Own Technology* (BYOT) initiative that allows students to take their smart phones, laptops, e-book readers, and tablets to class for educational purposes. Students are required to connect their devices to PISD’s wireless network and comply with this Acceptable Use Policy and the Student Code of Conduct.

It must also be understood that the Internet is a global, fluid community, which remains largely unregulated. While it is an extremely valuable tool for educational research, there are sections that are not commensurate with community, school, or family standards. It is the belief of the Board that the Internet’s advantages far outweigh its disadvantages. The Princeton ISD Board of Education will, through its administrative staff, provide an Internet screening system which blocks access to a large percentage of inappropriate sites. It should not be assumed, however, that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications.

Additionally, access to the Internet and computer resources is a privilege, not a right. Therefore, users violating the Princeton ISD Board of Education’s acceptable use policy shall be subject to revocation of these privileges and potential disciplinary action.

PRINCETON ISD COMPUTERS AND NETWORK RESOURCES
STUDENT USE ACCEPTABLE GUIDELINES

Please read the following carefully. Violations of the Acceptable Use Guidelines may cause a student's access privileges to be revoked, disciplinary action and/or appropriate legal action may be taken.

Any student who utilizes the computer lab(s) or any computer equipment at the school as well as students who voluntarily bring their own devices to school must be aware of certain policies for use of the equipment, network, and/or facilities. Procedures are in place for the protection of students and equipment. Students will be held accountable for any violation of the following policies (as would be the case for any classroom disciplinary matter).

As new technologies continue to change the world in which we live, they also provide many new and positive educational benefits for classroom instruction. To encourage this growth, Princeton ISD students may bring their own personal technology devices such as smart phones, laptops, e-book readers, and tablets to school. Responsibility to keep these devices secure rests with the individual owner. Princeton ISD is not liable for any device stolen or damaged on campus. Students are responsible for ensuring that any computers or digital devices, CDs, USB flash drives, or other forms of storage media that they bring in from outside the school are virus free and do not contain any unauthorized or inappropriate files. Students are permitted to use their device in the classroom ONLY if the device is used as an educational tool and ONLY if the use of the device is applicable to specific activities conducted in class (i.e., notes, calendar, research, calculator, e-readers, photos, and videos.) Students must notify teachers prior to taking pictures or videos in class. Any other classroom use of digital devices is considered a privilege and must be approved by the classroom teacher (i.e., games, apps, phone calls, texting, email, Facebook, Twitter). Outside of the classroom, (i.e., before school, hallways, lunch, after school) students are permitted to use their devices without restrictions as long as they adhere to the guidelines with this Acceptable Use Policy and the PISD Code of Conduct.

Students are required to connect to the district network via the secure wireless connection provided by the school system, but all access must be in accordance with this Acceptable Use Policy. Students are NOT permitted to use their own computing devices to access the Internet via personal Wi-Fi accounts or by any manner other than connecting through the secure wireless connection provided by the school system.

Safety Issues:

1. Never provide last name, address, telephone number, or school name online.
2. Never respond to, and always report to the teacher or parent, any messages that make you feel uncomfortable or that are from an unknown origin.
3. Never arrange a face-to-face meeting with someone you met on-line.
4. Never open attachments or files from unknown senders.
5. Always report to a teacher any inappropriate sites that you observe being accessed by another user or that you browse to accidentally.
6. In situations where earphones/ear buds are permitted to be worn inside or outside of the classroom, one ear bud must be left out in order to hear instructions given in class, in the halls, in the cafeteria, and other areas of school life.

Examples of prohibited conduct include but are not limited to the following:

A. Accessing, sending, creating or posting materials, pictures, videos, or communications that are:
    1. Damaging to another person's reputation,
    2. Abusive,
    3. Obscene,
    4. Sexually oriented,
    5. Threatening or demeaning to another person,
    6. Contrary to the school's policy on harassment,
    7. Harassing, or

8. Illegal

B. Posting or plagiarizing work created by another person without their consent.
C. Posting anonymous or forging electronic mail messages.
D. Attempting to read, alter, delete, or copy the electronic mail messages of other system users.
E. Giving out personal information such as phone numbers, addresses, driver's license or social security numbers, bankcard or checking account information.
F. Using the school's computer hardware or network for any illegal activity such as copying or downloading copyrighted software, music or images, or violation of copyright laws.
G. Using the school's computers or personal technology devices for cheating on an assignment or a test.
H. Downloading, installing, or using games, music files, public domain, shareware or any other unauthorized program on any school's computer or computer system.
I. Purposely bringing on premises or infecting any school computer or network with a Virus, Trojan, or program designed to damage, alter, destroy or provide access to unauthorized data or information.
J. Gaining access or attempting to access unauthorized or restricted network resources or the data and documents of another person.
K. Using or attempting to use the password or account of another person or utilizing a computer while logged on under another user's account.
L. Using the school's computers or network while access privileges have been suspended.
M. Using the school's computer hardware, network, personal devices, or Internet link in a manner that is inconsistent with a teacher's directions and generally accepted network etiquette.
N. Altering or attempting to alter the configuration of a computer, network electronics, the operating system, or any of the software.
O. Attempting to vandalize, disconnect or disassemble any network or computer component.
P. Utilizing the computers and network to retrieve information or run software applications inconsistent with school policy.
Q. Providing another student with user account information or passwords.
R. Connecting to or installing any computer hardware, components, or software which is not school system property to or in the district's technology resources without prior approval of the district technology supervisory personnel. Students are permitted to connect to the district network via the secure wireless connection provided by the school system, but all access must be in accordance with this Acceptable Use Policy. Students are NOT permitted to use their own computing devices to access the Internet via personal Wi-Fi accounts or by any manner other than connecting through the secure wireless connection provided by the school system.
S. Bringing on premises any computer, digital device, or storage device that contains a software application or utility that could be used to alter the configuration of the operating system or network equipment, scan or probe the network, or provide access to unauthorized areas or data.
T. Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.
U. Possessing or accessing information on school property related to "Hacking", or altering, or bypassing network security or policies.
V. Viewing a web site that is not age appropriate or a web site containing inappropriate materials.

Student Violation Consequences

Violation of PISD's policies and procedures concerning the use of computers and networks will result in the same disciplinary actions that would result from similar violations in other areas of PISD life. Any or all of the following consequences may be employed:

1. Loss of computer privileges/Internet access.
2. Any campus based disciplinary consequence permitted by the Student Code of Conduct.
3. Restitution for costs associated with system, hardware, or software restoration.

STUDENT PISD ACCEPTABLE USE OF COMPUTERS AND NETWORKS AGREEMENT

In order to make sure that all members of the PISD community understand and agree to these acceptable use guidelines, PISD requires that you and a parent/guardian sign the following statement.

I, (Please print student's name) ____, have read and understand the PISD Guidelines for Acceptable Use of Computers and Networks and Violation Consequences. I will abide by the Guidelines in letter and spirit, and understand that violating them may result in disciplinary action permitted by the Student Code of Conduct.

I also understand that PISD does not warrant that computers or networks will be error-free or uninterrupted; nor shall it be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, or profits) sustained or incurred in connection with the use, operation, or inability to use the system.

I understand that, though there is a great wealth of educational information on the Internet, there is also objectionable material on the Internet. I understand that, while all precaution from PISD staff will be taken to prevent access from these sites, accidental access cannot be guarded against completely. It should not be assumed that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications. I will not hold the district responsible for materials accessed. Place a check mark on the lines that apply below.

____ I give permission for my child to **access the Internet** through PISD connections.

____ I deny permission for my child to **access the Internet** through PISD connections.

Date:_____________

School: ____

Student Name (Please print):______________________________________

Student's Signature:____

Parent or Guardian Name (Please print): ____________________________

Parent or Guardian Signature:______________________________________

This form will be retained on file for one school year.

Please sign this page and return it to the student's school. Thank you.

EMPLOYEE PISD ACCEPTABLE USE OF COMPUTERS AND NETWORKS AGREEMENT

In order to make sure that all members of the PISD community understand and agree to these acceptable use guidelines, Princeton ISD requires that you sign the following statement:

I, (Please print employee name) ____, have read and understand the
PISD Guidelines for Acceptable Use of Computers and Networks as well as the Princeton ISD Employee Handbook regarding the use of technology. I will abide by the Guidelines in letter and spirit, and understand that violating them may result in disciplinary action.

I also understand that PISD does not warrant that computers or networks will be error-free or uninterrupted; nor shall it be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, or profits) sustained or incurred in connection with the use, operation, or inability to use the system.

Date:_____________

School: ____

Employee Name (Please print):_____________________________________

Employee Signature: ____

This form will be retained on file for one school year.