

Pflugerville I.S.D. Acceptable Use Policy

Acceptable Use

The District's technology resources will be used only for learning, teaching and administrative purposes consistent with the District's mission and goals. The District will make copies of the acceptable use guidelines available to all users.

Access to the District's Electronic Communications System is a privilege not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with district policies. (Student Code of Conduct and Administrative Procedures Manual)

A student knowingly accessing or bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly accessing or bringing prohibited materials into the schools electronic environment will be subject to disciplinary action in accordance with District policies.

Access Availability

Access to the District's Electronic Communications System including the Internet shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use;

1. imposes no tangible cost on the district;
2. does not unduly burden the district's computer or network resources; and
3. has no adverse effect on the employee's job performance or on a student's academic performance.

Public Access

Access to the District's Electronic Communications System including the Internet shall be made available to members of the public, in accordance with administrative regulations. Such use may be permitted so long as the use:

1. imposes no measurable cost on the district; and
2. does not unduly burden the district's computer or network resources.

Monitored Use

Student use of the computers and computer network is only allowed when supervised by staff members.

Electronic mail transmissions and other use of the electronic communication system by students and employees shall not be considered private. Designated District staff shall be authorized to monitor such communication at any time to ensure appropriate use.

Network

Improper or illegal use of any computer or the network is prohibited. This includes the following:

- Using racist, profane, or obscene language or objectionable materials
- Attempting to or harming equipment, materials or data
- Attempting to or sending anonymous messages of any kind
- Using the network to access inappropriate material
- Knowingly placing a computer virus on a computer or the network
- Using the network to provide addresses or other personal information that others may use inappropriately
- Accessing of information resources, files and documents of another user without their permission

Modified June 30, 2012

Deleting outdated files on a regular basis is required of all Users.

Security

You may not share your account with anyone or leave the account open or unattended. Attempting to log on or logging on to a computer or email system by using another's password is prohibited. Assisting others in violating this rule by sharing information or passwords is unacceptable. Users will change passwords regularly using combinations of letters and numbers.

Users are responsible for saving all documents to the server. Department of Technology staff will attempt to recover documents only if they have been saved to the server.

Internet Safety / Filtering

The District adheres to the federal Children's Internet Protection Act Guidelines. (CIPA) The District network maintains a filtering device that blocks access to visual depictions that are obscene, pornographic, inappropriate for students or harmful to minors as defined by the federal CIPA. The District shall enforce the use of such filtering devices and shall not authorize the disabling of a filtering device for any reason. The following are in place to protect students' Internet use.

1. Students access to inappropriate materials is controlled through the Internet filter.
2. The district's private email system does not allow outside access to the directory of names. Instant Messaging is restricted to Intranet chats.
3. Students are not allowed to reveal personal address or phone number information when using the electronic communication system.
4. Chats using the district email system will be supervised and monitored.
5. Students may participate in prearranged Internet chats with experts that have been scheduled by PISD staff.
6. Access to social media and Web 2.0 content is accessible by staff provided proper review of all content is done prior to use and distribution in classrooms.
7. Staff usage of social media shall include the creation of a classroom centered page that does not interact with personal pages or feeds.

The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Although the district will use these preventative practices, system users and parents should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

Copyright

All users are responsible for adhering to existing copyright laws pertaining to software, resources, references, video, sound and graphics. Users will cite their source of information. Questions concerning copyright can be referred to the campus or district administrative staff.

Email

1. Email cannot be used for private or commercial offerings of products or services for sale or to solicit products or services.
2. Email cannot be used for political or religious purposes.
3. Email will be deleted regularly to conserve server file space.
4. Email messages that cause network congestion or interfere with the delivery of mail to others are not acceptable.
5. Email from list serves must not affect the server's performance.
6. Students will not access Web based email accounts.

System users are to observe the following network etiquette.

7. Be polite. Messages typed in capital letters are considered rude.
8. Email messages and conference postings will not contain improper language, swearing, vulgarity, ethnic or racial slurs or any other inflammatory language. Conference postings will follow the District guidelines or be removed.

Modified June 30, 2012

9. Do not reveal personal information of users or others.
10. Do not send chain letters, or forward messages to large groups of users.
11. Users are responsible for material delivered to their accounts.
12. Mail from outside email providers must meet the District Acceptable Use Policy.

Forgery

Forgery or attempted forgery of electronic data is prohibited. Attempts to read, delete, copy, or modify the electronic data or the deliberate interference with an electronic system is prohibited.

Software

Please contact the District Technology Department to install or reinstall any software on District computers. The illegal installation of copyrighted software or files, on District computers is prohibited. Only software approved, licensed and or purchased by the District should be installed on District computers.

Vandalism

Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, hardware, or software costs.

Disclaimer

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on, the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the district.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

If you have questions or need further information, please contact the campus principal.

Signature

Date