

**Pittsburg Community School District
Administrative Guidelines for Board of Education
"Student Acceptable Use Policy"**

This policy is written and maintained by the system administrator and the administration of Pittsburg Unified School District #250. If you have any comments regarding this policy, please contact the district technology office.

Unauthorized usage of the district's computing systems may involve not only transgression of district policy, but also a violation of state and federal laws. Unauthorized use is a crime and may involve criminal and civil penalties.

For the purposes of these guidelines, communication technologies include the Internet (i.e. World Wide Web (WWW)), on-line services, e-mail, other internet-related services, district provided computers, phones, and school district computer networks, and other applicable services or technologies either now in use or implemented in the future. Communication technologies include technologies (whether or not owned by the school district) in use on school grounds or at school activities.

The system administrator reserves the right to disable any account, at anytime, in the event of a real or perceived infraction until further notice.

Student Rights and Responsibilities

Student's use of communication technologies is a privilege intended for the educational benefit of the student. Students must comply with the terms of these guidelines, any applicable district board policies, administrative guidelines, and operating procedures relative to the use of communication technologies. In using communication technologies, the student will follow these guidelines:

- A. No student on this system shall operate in any fashion as to impede the use of said system by ANY other user, regardless of class or group membership.
- B. If any user finds another user of the system to be in violation, or suspicion of violation of any rules or policies, the finding user is to notify the system administrator, building administrator, or classroom teacher immediately, and WILL NOT attempt to police this system on his/her own.
- C. The sharing of accounts with friends or relatives is strictly prohibited without prior permission from the system administrator.
- D. The running of ANY software that was not installed by the system administrator or his agents is prohibited without prior consent of the system administrator.
- E. Adult material is strictly prohibited.
- F. Users are responsible for all activities associated with their accounts. If a user releases their password to a third party who violates system policy, the owner of the account WILL BE RESPONSIBLE.
- G. Use of this system is a privilege, not a right. Severe misuse or repeated infractions will result in a temporary or permanent loss of use and the user may be subject to other disciplinary actions.

Unacceptable and Inappropriate Use

The following forms of use of communication technologies are unacceptable and inappropriate and will be considered violations of board policy and administrative guidelines. Violators may be subject to disciplinary actions which may including the temporary or permanent loss of use of technology and even suspension. Examples of unacceptable\inappropriate use for a student include:

- A. Creating, coping, knowingly distributing, or posting of a computer virus;
- B. Sending messages using someone else's account;
- C. Sending messages that are inconsistent with district rules;
- D. Sending a message that is sexist, racist, or otherwise prejudicial or inflammatory;
- E. Sending messages or downloading files that knowingly contain obscene language, graphics, pictures, or attached graphics files, either encoded/encrypted or un-encoded/decrypted;
- F. Sending chain letter-type messages that are not related to education through email or chat;
- G. Engaging in online chat sessions that are not related to school functions;
- H. Using school provided technologies for personal gain;
- I. Sharing of account and/or password with others;
- J. On-line use of obscene, harassing or abusive language;

- K. Attempting to gain access to inappropriate websites;
- L. Attempting to log-in to district computer networks as a network administrator;
- M. Accessing or attempting to access any part of the district computer networks or any part of a sub-system of the Internet without proper authorization;
- N. Theft or intentional destruction of district equipments.
- O. Plugging in or unplugging Ethernet cables or to move computers or printers without approval from system administration.
- P. Use communication technologies in any way that violates school rules, administrative guidelines, Board policies or procedures, state statutes, local ordinances, or other laws.

Consequences of Unacceptable Use

In the event that an infraction is discovered or reported, the offending user will be promptly notified and given a chance to discuss the action with the system administrator and district and/or building administration depending on the severity of the infraction.

The offending student may be temporarily barred from technology usage pending investigation. Emails provided through district email services considered to be private information. Only under the most severe of circumstances will user email be read.

Network Storage Usage

The school district provides server space for students to store files and data that are for school purposes only. All accounts have a file system quota of 20MB. This limit may be exceeded to limit of 40MB for a short period of time for downloading, but any data that is in excess of the 20MB limit is subject to being erased. Students should backup their data regularly in the event of server failure or loss of data. If a student is in need of more space, contact the system administrator. Quotas may be increased temporarily and for special purposes.

Logs and Monitoring

The communication technologies provided in the district are owned and monitored by the systems administrator including, but not limited to files stored or transmitted, emails, and use of terminals. The district system creates logs of most user activity. These logs can be used as evidence of unauthorized usage. The system administrator may also monitor the input from any terminal, at any time in the event of suspected unauthorized use, or use that is not consistent with district or system policy. The system administrator is sworn to secrecy in the event that private information that is not in violation of policy is monitored.

Last Update: March 27, 2009

Student Signature

Date