

## 2361 ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

The Board of Education recognizes that as telecommunications and other new technologies shift the manner in which information is accessed, communicated and transferred that those changes will alter the nature of teaching and learning. Access to telecommunications will allow pupils to explore databases, libraries, Internet sites, bulletin boards and the like while exchanging information with individuals throughout the world. The Board supports access by pupils to information sources but reserves the right to limit in-school use to materials appropriate to educational purposes. The Board directs the Superintendent to effect training of teaching staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The Board also recognizes that telecommunications will allow pupils access to information sources that have not been pre-screened by educators using Board approved standards. The Board therefore adopts the following standards of conduct for the use of computer networks and declares unethical, unacceptable or illegal behavior as just cause for taking disciplinary action, limiting or revoking network access privileges and/or instituting legal action.

The Board provides access to computer network/computers for educational purposes only. The Board retains the right to restrict or terminate pupil access to the computer network/computers at any time, for any reason. The Board retains the right to have district personnel monitor network activity, in any form necessary, to maintain the integrity of the network and ensure its proper use.

### Standards for Use of Computer Networks

Any individual engaging in the following actions when using computer networks/computers shall be subject to discipline or legal action:

- A. Using the computer network(s)/computers for illegal, inappropriate or obscene purposes, or in support of such activities. Illegal activities are defined as activities that violate federal, state, local laws and regulations. Inappropriate activities are defined as those that violate the intended use of the network. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles.
- B. Using the computer network(s)/computers to violate copyrights, institutional or third party copyrights, license agreements or other contracts.



- C. Using the computer network(s) in a manner that:
1. Intentionally disrupts network traffic or crashes the network;
  2. Degrades or disrupts equipment or system performance;
  3. Uses the computing resources of the school district for commercial purposes, financial gain or fraud;
  4. Steals data or other intellectual property;
  5. Gains or seeks unauthorized access to the files of others or vandalizes the data of another user;
  6. Gains or seeks unauthorized access to resources or entities;
  7. Forges electronic mail messages or uses an account owned by others;
  8. Invades privacy of others;
  9. Posts anonymous messages;
  10. Possesses any data which is a violation of this policy; and/or
  11. Engages in other activities that do not advance the educational purposes for which computer networks/computers are provided.

## Internet Safety/Protection

The school district is in compliance with the Children's Internet Protection Act and has installed technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter visual depictions that are obscene as defined in Section 1460 of Title 18, United States Code; child pornography, as defined in Section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.



The school district will certify on an annual basis, that the school, including media centers/libraries, in the district are in compliance with the Children's Internet Protection Act and the school district enforces the requirements of this policy.

This Policy also establishes Internet safety policy and procedures in the district as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding blocking and/or filtering the visual depictions prohibited in the Children's Internet Protection Act, the Board shall determine other Internet material that is inappropriate for minors. The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly board meeting or during a designated special board meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 2361.

## System Security

Users are responsible for their accounts and should take all reasonable precautions to prevent unauthorized access to them. In no case should a user provide his/her password to another individual.

Users shall immediately notify the supervising staff person or data processing department if they detect a possible security problem. Users shall to access the system for the purpose of searching for security problems.

Users shall not install or download software or other applications without permission of the supervising staff person.

Users shall follow all district virus protection procedures when installing or downloading approved software.

## Consent Requirement

No pupil shall be allowed to use the computer network and the Internet unless they shall have filed with the Main office a consent form signed by the pupil and his/her parent(s) or legal guardian(s).



## Violations

Individuals violating this policy shall be subject to the consequences as indicated in Regulation No. 2361 and other appropriate discipline, which includes but are not limited to:

1. Use of the network only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension from school;
7. Expulsion from school; and/or
8. Legal action and prosecution by the authorities.

N.J.S.A. 2A:38A-3  
Federal Communications Commission: Children's Internet  
Protection Act.

Adopted: 27 July 2009

