TOWNSHIP OF ELK BOARD OF EDUCATION

100 UNIONVILLE ROAD GLASSBORO, NJ

POLICY NO. 2340

ACCEPTABLE USE POLICY OF NETWORK COMPUTERS AND RESOURCES BY STAFF MEMBERS

The Board 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 teachers to explore databases, libraries, Internet sites, bulletin boards and the like while exchanging information with individuals throughout the world. The Board supports access by teachers to information sources but reserves the right to limit in-school use to materials appropriate to educational purposes in an elementary setting. The Board directs the Superintendent to develop 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 teachers 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 staff-member 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 insure its proper use.

Internet Access

Because the school district provides, through connection to the Internet, access to other computer systems around the world, teachers must understand that the Board and system administrator have no control over content. While most of the content available on the Internet is innocuous and much of it a valuable educational resource, some objectionable material exists. The Board will allow pupil access to Internet resources only under direct teacher supervision. Each teacher is morally and professionally responsibility to ensure that student Internet use is for a legitimate educational purpose. **Unrestricted searches or "surfing" of the Internet by students is expressly forbidden.**

Teachers are advised that some systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal material. The Board and the system administrator do not condone the use of such materials and do not permit usage of such materials in the school environment. Staff members knowingly bringing such materials into the school environment will be disciplined in accordance with Board policies and regulations and such activities may result in termination of such staff member's access on the computer network.

Software Libraries on the Network

Software libraries on the network are provided to teachers as an educational resource. No one may install, upload, or download software without the expressed consent of the system administrator. Any software having the purpose of damaging other members' accounts on the school district computer network/computers (e.g., computer viruses) is specifically prohibited. The system administrator, at their sole discretion, reserve the rights to refuse posting of files and to remove files. The system administrator, at their sole discretion, further reserves the right to immediately limit usage or terminate the account or take other action consistent with the Board's policies and regulations of a member who misuses the software libraries.

Electronic Mail

Electronic Mail "e-mail" is provided by the Board to enhance professional communications.

All messages sent and received on the school district computer network must have an educational purpose and are subject to review. Messages received by the system are retained on the system until deleted by the recipient or for a maximum of 15 days. A canceled account will not retain its E-mail. Staff members are expected to remove old messages within 15 days or the system administrator may remove such messages. The system administrator may inspect the contents of E-mail sent by one staff member to an addressee, or disclose such contents to other than the sender or a recipient when required to do so by the Board policy, regulation, or other laws and regulations of the State and Federal governments. The Board reserves the right to cooperate fully with local, state, or federal officials in any investigation concerning or relating to any E-mail transmitted on the school district computer networks or computers.

Disk Usage

The system administrator reserves the right to set quotas for disk usage on the system. A staff member who exceeds his/her quota of disk space will be advised to delete files to return to compliance with predetermined quotas.

Security

Security on any computer system is a high priority, especially when the system involves many users. If a staff member feels that he/she can identify a security problem on the computer network, the staff member must notify the system administrator. The staff member should not

inform individuals other than the system administrator of a security problem. Staff members may not allow others to use their account and password. Attempts to log on to the system using another staff member's account or as a system administrator will result in termination of the account. Staff members should immediately notify a system administrator if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any staff member identified as a security risk will have limitations placed on usage of the computer network/computers or may be

terminated as a user and is subject to other disciplinary action. Students are not permitted to log on to the network under a staff member's password.

Printing

The printing facilities of the computer network/computers should be used judiciously. Printing for other than educational purposes is prohibited.

Standards for Use / Misuse of Computer Networks:

Any individual engaging 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 which 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 network/computers are provided.

Violations:

Staff members violating this policy shall be subject to consequences and other appropriate discipline which includes, but is 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. Possible Administrative and/or Board discipline;

7. Legal action and prosecution by the authorities;

Adopted: 11/21/97

Revised: 09/11/97

Revised: 05/14/98