ADMINISTRATIVE PROCEDURES

ADULT USE OF NETWORKED RESOURCES

The North East School District ("District") provides network resources to members of its administration, faculty, staff, volunteers, and other adults ("adult users") in order to facilitate communications in support of research and education. The District anticipates that electronic mail, the Internet, and other telecommunications devices ("networked resources") will expedite the sharing of effective practices, lessons and other education-related information across the District and will help adult users to stay on the leading edge of education by forming partnerships with others across the nation and around the world. In furtherance of these goals and objectives, it is the policy of the District to maintain an environment that promotes ethical and responsible conduct in the use of networked resources by adult users. Through this and other policies, it is the intent of the District to comply with the provisions of the Children's Internet Protection Act ("CIPA").

I. General Expectations for Adult Use of Network Resources

The District expects adult users to utilize networked resources in a professional and responsible manner. However, with access to computers and people all over the world, it is inevitable that adult users will encounter material that may not be appropriate for the educational environment. The District will attempt to limit the access to such material by maintaining and enforcing a technology protection measure with respect to all of its computers having access to networked resources.

The technology protection measure will, to the greatest extent possible, block or filter access through networked resources to visual depictions that are obscene, contain child pornography, or are otherwise inappropriate. Adult users should not send or open communications through the network that may be harmful to minors. However, because no technology protection measure is effective completely, adult users should be aware that inappropriate materials could be encountered during legitimate research or communications. If inappropriate material is inadvertently encountered, it must be disengaged from immediately and removed from the network. If necessary, technical assistance should be obtained to do so.

Adult users may not utilize networked resources for the unauthorized disclosure, use or dissemination of confidential personally identifiable information regarding students or other employees.

II. Supervision of Students' Use of Network Resources

Adult users will oversee the use of network resources by students under their supervision to ensure that students adhere to the District's Computer/Internet Acceptable Use Policy for Students. Consequently, adult users should familiarize themselves with the requirements set forth in that policy.

Notwithstanding the existence of technology protection measures, the breadth of networked resources make it possible that students could access obscene, pornographic, or otherwise inappropriate materials. Adult users will monitor student use of network resources and shall disengage obscene, pornographic or otherwise inappropriate materials immediately and remove them from the network. If necessary, technical assistance should be obtained to do so.

III. District Supervision of the Use of Networked Resources

The District has a legal obligation to assure that its networked resources are utilized in a manner consistent with its goal of providing a safe and healthy educational environment for its students. This interest applies equally to student use and adult use of networked resources. Therefore, adult users must understand that the District provides no networked resources for the sending and receiving of personal, private, or confidential electronic communications. The Technology Coordinator has access to all mail and may examine messages to ensure compliance with law and this policy. Electronic mail messages may be subject to subpoena. Messages and/or activities relating to and in support of illegal activities are prohibited and will be reported to the appropriate authorities. The District reserves the right to monitor the use of networked resources.

IV. Security

Security on any network is a high priority, especially when the network involves many users. If an adult user identifies a security problem on the network, he/she should notify the Technology Coordinator immediately. Adult users should not demonstrate the problem to other users.

Adult users must not use another individual's network account without their written authorization. Adult users must not reveal their password to anyone. Adult users must not attempt to log on to the network as the Technology Coordinator. Any adult user identified as a security risk or having a history of problems with other network systems may be denied access to the network resources.

Adult users may not download or install any commercial software, shareware, or freeware to the District network, unless specifically authorized to do so by the Technology Coordinator. District computers may be audited and unauthorized or unlicensed software will be removed.

Adult users must not open electronic mail or other communication from suspicious or unidentified sources. In the event that an adult user receives a communication containing a virus or other self-perpetuating program that is potentially harmful or disruptive to the network, the adult user should report the incident immediately to the Technology Coordinator.

V. Prohibited Activities

The Use of the District's Networked Resources is a Privilege, Not a Right.
Inappropriate use of networked resources, including any violation of this policy, may result in cancellation of the privilege and, in the case of District employees, disciplinary action.

The following activities are strictly prohibited on the District's network:

A. The use of the network for commercial or for-profit purposes,

B. The use of the network for political lobbying,

C. The unauthorized use of a network account by anyone but the owner of the account,

D. The unauthorized acquisition of information on other users, obtaining of copies of data belonging to other users, modification of files of other users, or acquisition and/or use of passwords belonging to other users,

E. The intentional disruption of the network and/or network resources, including the creation, facilitation and/or perpetuation of "chain letters" or similar forms of broadcast mail,

F. The destruction, modification, or abuse of network hardware or software,

G. The use of networked resources to develop programs that harass, insult, or attack other users, infiltrate a computer or network and/or damage the software components of a computer or network (i.e. deliberately introducing a virus into the network; "hacking"),

H. The use of profanity or inappropriate language in electronic mail or other network communication,

I. The downloading or uploading of pirated or illegal software in violation of copyright law and/or the reproduction of copyrighted material without the express permission of the author/copyright owner,

J. The use of networked resources to access or process obscene material, material relating to any type of pornography, inappropriate text files, or files dangerous to the integrity of the network,

K. The unauthorized disclosure, use, or dissemination of personal or confidential information on students and/or other employees,

L. The use of networked resources by an adult user to give the false impression that he/she represents the District in a given capacity, and

M. The transmission of any material in violation of federal or state law.