453 & 524 - ACCEPTABLE USE OF NETWORKED INFORMATION RESOURCES

I. PURPOSE

The purpose of this policy is to provide direction for development of school district policies and guidelines for acceptable use of networked resources.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding user access to networked resources, District 206 considers its own stated educational mission and goals. Telecommunications, electronic information sources and networked services significantly alter the information landscape for schools by opening classrooms to a broad array of resources. Electronic information research skills are now fundamental to preparing citizens and future employees. Access to networked resources will enable users to explore thousands of libraries, databases, bulletin boards, and other resources. District 206 staff will blend thoughtful use of networked information throughout the curriculum and provide guidance and instruction to students in its use.

III. RESPONSIBILITY

A. The school board recognizes the expertise of professional staff and the vital need of such staff to be primarily involved in recommending acceptable use policies and guidelines. Accordingly, the school board directs the superintendent and professional staff to formulate recommendations to the school board on acceptable use policies and guidelines.

B. In developing recommendations for acceptable use policy guidelines, the professional staff shall write specific acceptable use policy rules, guidelines and enforcement procedures that:

1. Describe general instructional philosophies and strategies to be supported by access to networked resources in schools.

2. Describe sanctions to be taken when violations of the policy occur.

3. Describe the process for governing network system security, user accounts and user privileges for students, staff, and faculty.

4. Make specific reference to prohibiting the use of school district networked resources to:

a. Provide, assist in, or gain unauthorized or inappropriate access to the district's technology resources, with regards to voice, video, or data.

b. Interfere with the ability of students/staff members to use the district's technology resources or other network connected services effectively.

c. Gain unauthorized access to another students/staff member's work or engage in activities that result in the loss of another student/staff members work.

d. Distribute any material in such a manner that might cause congestion of the voice, video, and data networks.

e. Access, distribute or collect obscene, abusive or threatening material via telephone, video, electronic mail, Internet or other means.

f. Use technology resources for a commercial, political, or profit-making enterprise, except as specifically agreed to with the district.

5. Integrate acceptable use policy with other district policies such as those concerning:

a. Copyright Policy (#718)

b. Policy regarding Harassment and Violence (#413)

c. Selection and Review of Instructional Materials (#632)

e. Hazing Policy (#507)

f. Districtwide Student Discipline Policy (#506)

6. School districts which receive certain federal funding, such as e-rate discounts, for purposes of Internet access and connection services and/or receive funds to purchase Internet accessible computers are subject to the federal Children's Internet Protection Act, effective in 2001. This law requires school districts to adopt an Internet safety policy which contains the provisions set forth below. Also, the Act requires such school districts to provide reasonable notice and hold at least one public hearing or meeting to address the proposed Internet safety policy prior to its implementation. The following alternative language for school districts that seek such federal financial assistance satisfies both state and federal law requirements.

A. With respect to any of its computers with Internet access, the School district will attempt to filter the online activities of minors and employ technology protection measures during any use of such computers by minors and adults. The technology protection measures utilized will attempt to block or filter Internet access to any visual depictions that are:

1. Obscene,
2. Child pornography, or
3. Harmful to minors.

B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or

2. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

7. Require that users, and where appropriate their parents or guardians, be notified of the guidelines and policies governing the use of district network resources. This notification should include:

a. Disclaimers limiting the school district's liability relative to:

(1) Information stored on school district electronic digital media, hard drives or servers.

(2) Information retrieved or sent through school district computers, networks or online resources.

(3) Personal property used to access or connect with school district computers, networks or online resources.

(4) Unauthorized financial obligations resulting from use of school district resources/accounts to access networked resources.

b. Notification that, even though the school district may use technical means to limit student access to networked resources, these limits do not provide a foolproof means for enforcing the provisions of local acceptable use policies.

c. Notification that electronic messages and files stored on electronic devices, computers, servers, communications via electronic mail, Internet browsers or voice mail are not private.

d. Notification that all data and other material and files maintained on the school district system may be subject to review, disclosure, or discovery under the Minnesota Government Practices Act.

IV. GUIDELINES FOR ACCEPTABLE USE OF NETWORK RESOURCES

A. Enforcement of the Policy

1. Teachers and building administrators have responsibility for enforcing the district's policy on "Acceptable Use of Networked Information Resources" with students.

2. Building and district administrators have responsibility for enforcing the district's "Acceptable Use Policy of Networked Information Resources" with staff.

B. Consequences of Breach of Policy

The use of technology resources is a privilege, not a right. The district recognizes that some personal use of the electronic mail system, voice mail and computer systems by students and staff - including use during non-work time is acceptable. However, excessive use or abuse of these privileges [as outlined in Section III of the Acceptable Use Policy] is unacceptable. For students and staff, excessive personal use and or abuse of these privileges may result in one or more of the following consequences:

1. Suspension or cancellation of use or access privilege.

2. Payments for damages, repairs or labor for restoration.

3. Discipline under appropriate school district policies including:

(a.) Suspension

(b.) Expulsion

(c.) Exclusion or termination of employment.

(d.) Civil or criminal liability under applicable laws.

C. Building Additions to the Guidelines

Building staff who wish to make additions to these guidelines must notify the Director of Technology in writing. Any proposed additions should in no way negate or impinge on the user responsibility and unacceptable use set forth in the "Acceptable Use Policy of Networked Information Resources." It will be the district's policy to grant all requests that fit within the planning for content, performance, use and security of the networks.

D. Privacy

1. By authorizing use of technology resources, District 206 does not relinquish control over materials on the systems or contained in files on the systems. Files stored on school-based computers, servers, electronic media and

communications via electronic mail, Internet browsers or voice mail are not private.

2. Electronic messages and files stored on school-based computers, servers, and electronic media may be treated like any other school property. Administrators, staff, or network personnel may review files and messages to maintain system integrity and, if necessary, to insure the users are acting responsibly.

3. District 206 employees and students should also be aware that data and other material and files maintained on school-based computers, servers and electronic media may be subject to review, disclosure, or discovery under Minnesota Government Practices Act. The school district will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.

4. Employees are also discouraged from excessive use of the district's electronic mail, voice mail, and computer systems for personal use. Excessive or inappropriate personal use of the electronic communications systems may result in disciplinary action.

V. SPECIFIC RULES AND BEST PRACTICES FOR ACCEPTABLE USE OF NETWORK RESOURCES

District 206's Wide Area Network infrastructure, as well as the building-based Local Area Networks have been implemented with performance planning as a major part of the process along with appropriate security. Guarantee of an appropriate level of network efficiency is one of the foremost priorities of the Technology Department along with acceptable use practices and best use of resources.

To that end, modifications to an individual building network infrastructure and use will almost always affect Local Area Network performance and quite often will have an impact on the efficiency of the Wide Area Network. For these reasons, consider the following issues before instigating any changes to a building network infrastructure or use. With any change, it is necessary to work with the Director of Technology.

A. Passwords

All users that have access to building and district servers must maintain a password for their account. Users are responsible for the safekeeping of their passwords. Passwords will be changed upon request from either staff or a district technology specialist. The passwords shall be a minimum of 6 characters in length with at least one of the characters being a number or special character.

B. Student Use of Wireless Networks & Internet

Students utilizing district-provided Wireless Networks & Internet access must have permission. Students utilizing district-provided Wireless Networks & Internet

access are responsible for good behavior on-line just as they are in a classroom or any other part of the school. The same general rules for behavior and communications apply. Parents/Guardians must approve student Wireless Network & Internet access use as follows:

- Elementary Students – once in kindergarten and for any new student.
- Secondary Students – once in grade 7 and for any new student.
- Parents/guardians may restrict their student's access by informing the school district in writing.

C. Electronic Mail

Electronic mail is an electronic message sent by or to a staff member or students, for business or instructional communications purposes. Following are electronic mail guidelines:

1. Messages received by the electronic mail system are retained on the system until deleted by the recipient.

2. Students and staff members are expected to remove old messages in a timely fashion.

3. The system administrators may remove old messages.

4. The system administrator will not intentionally inspect the contents of electronic mail or disclose such contents to other than the sender or intended recipient without the consent of the sender or intended recipient unless required to do so by law or District 206 policy or to investigate complaints regarding electronic mail which is alleged to contain material contrary to district policy.

5. Accounts for students and staff members may be requested through the building electronic mail contacts.

6. Individual student accounts for electronic mail will not be issued except as discussed in Item V-B.

D. Use of E-Mail

Procedures for the use of e-mail are detailed in Policy #623 (Use of E-mail).

VI. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district's network & systems is at the user's own risk. The network & systems are provided on an "as is, as available" basis. The school district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage, or unavailability of data stored on school district storage media or servers or for delays or changes in or interruptions of services or mis-deliveries or non-deliveries of information or materials, regardless of the cause. The school district will not be responsible for damages

to personal devices connected to the district's network or system no shall the district be responsible for any financial obligations arising through unauthorized use of the school district system or internet.

Policy Adopted: 9/18/95
Revised: 4/18/05, 7/17/06, 12/12
Independent School District No. 206
Alexandria, Minnesota