Adopted: June 21, 2004

Revised: December 5, 2011

524 INTERNET/~~INTRANET~~ ACCEPTABLE USE AND SAFETY POLICY

I. PURPOSE

The purpose of this policy is to ~~communicate the guidelines and policies of ISD 726 regarding access to and safe and acceptable use of both the district's computer systems as well as Internet/Intranet.~~ set forth policies and guidelines for access to the school district computer system and acceptable and safe use of the Internet, including electronic communications.

II. ~~EDUCATIONAL INTENT~~ GENERAL STATEMENT OF POLICY

~~Students and staff in District 726 have access to both the school's internal network and the Internet/Intranet. The district has provided these network services in order to allow students and staff access to a wide range of valuable informational and educational resources, including thousands of libraries, databases, research institutions and a multitude of other information sources that can be used to educate, inform and entertain. Electronic information research skills and information literacy skills are now fundamental to the preparation of citizens in a democracy. Staff and students are expected to limit their use of these school-provided resources to those activities that are educational and/or consistent with the district's mission statement. Students may use school computers to access non-school issued email accounts only for educational purposes and/or communication consistent with the district's mission and policy statements and with permission from media/technology staff. Uses that might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.~~

In making decisions regarding student and employee access to the school district computer system and the Internet, including electronic communications, the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school district computer system and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The school district expects that faculty will blend thoughtful use of the school district computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school district computer system, which includes Internet access and devices. The purpose of the system is more specific than providing students and employees with general access to the Internet. The school district system has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development activities. Users are expected to use Internet access through the district system to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

~~III~~ IV. USE OF THE SYSTEM AS A PRIVILEGE~~, NOT A RIGHT~~

~~Use of the Internet/Intranet is a privilege, not a right. Users are responsible for good behavior on the network just as they are in any other school setting. Access to network services will be provided to students who agree to act in a considerate and responsible manner. The District and its personnel have the right to restrict or terminate access to the Internet/Intranet at any time for just cause. At all times, user behavior should conform to other District policies, such as the Student Discipline Policy and the Sexual Harassment Policy. Consequences for the misuse of this resource will be determined on a case by case basis and may include loss of computer privileges, payments for damages and repairs, suspension, expulsion or other disciplinary action, termination of employment and/or civil or criminal liability under applicable laws. Infractions by users may also be referred to legal authorities when appropriate.~~ The use of the school district system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment; or civil or criminal liability under other applicable laws.

~~If a user accesses an inappropriate website inadvertently, the user should exit the site immediately and report the incident to the supervising adult. In the case of a school district employee, the disclosure should be to the employee's immediate supervisor. This disclosure may serve as a defense against an allegation of a policy infraction. Networking monitoring software may be used to determine the veracity of the student's defense.~~

~~IV~~. UNACCEPTABLE USES ~~OF THE NETWORK/INTERNET/INTRANET~~

~~Unacceptable uses of the Internet/Intranet include, but are not limited to, the following~~

A. The following uses of the school district system, devices, and Internet resources or accounts are considered unacceptable:

~~• Viewing, using or distributing inappropriate, abusive or obscene materials and/or language~~

~~• Viewing, using or distributing materials and/or language in a manner that advocates or promotes violence, hate literature, harassment, defamation or discrimination~~

~~• Revealing or posting personal information, such as addresses, and phone numbers, *(either the student's own or those of another individual*) on district or school-associated websites. The district does not prohibit employees from posting their school contact information on the school district or associated webpage's nor communications between employees and other users when such communications are made for education-related purposes.~~

~~• Engaging in activities that are illegal, including the violation of copyright and other laws~~

~~• Using the network to attempt to disrupt, damage or subvert its use by others, including knowingly spreading computer viruses, or in a way that results in the loss of another's work, or wastes network capacity~~

~~• Use of any external proxy service in attempt to bypass or thwart existing district content policies.~~

~~• Installing unauthorized software on school computers or downloading software or files~~

~~• Using an account owned by another person, with or without their permission, or permitting other students to use one's Internet/Intranet access or account~~

~~• Using the network for a commercial, political or profit-making enterprise~~

~~• Plagiarizing material from network resources~~

~~• Using the network in any way that violates any formal or informal school policies and behavior standards~~

1. Users will not use the school district system to access, review, upload, download, store, print, post, receive, transmit, or distribute:

a. pornographic, obscene, or sexually explicit material or other visual depictions that are harmful to minors;

b. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;

c. materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;

d. information or materials that could cause damage or danger of disruption to the educational process;

e. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

2. Users will not use the school district system to knowingly or recklessly post, transmit, or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

3. Users will not use the school district system to engage in any illegal act or violate any local, state, or federal statute or law.

4. Users will not use the school district system to vandalize, damage, or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software, or system performance by spreading computer viruses or by any other means, will not tamper with, modify, or change the school district system software, hardware, or wiring or take any action to violate the school district's security system, and will not use the school district system in such a way as to disrupt the use of the system by other users.

5. Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information, or files without the implied or direct permission of that person.

6. Users will not use the school district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable

information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs, or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

a. This paragraph does not prohibit the posting of employee contact information on school district webpages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).

b. Employees creating or posting school-related webpages may include personal contact information about themselves on a webpage. However, employees may not post personal contact information or other personally identifiable information about students unless:

(1) such information is classified by the school district as directory information and verification is made that the school district has not received notice from a parent/guardian or eligible student that such information is not to be designated as directory information in accordance with Policy 515; or

(2) such information is not classified by the school district as directory information but written consent for release of the information to be posted has been obtained from a parent/guardian or eligible student in accordance with Policy 515.

In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, employees shall obtain written approval of the content of the postings from the building administrator.

c. These prohibitions specifically prohibit a user from utilizing the school district system to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as "MySpace" and "Facebook."

7. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district

system, attempt to log in through another person's account, or use computer accounts, access codes, or network identification other than those assigned to the user. Messages and records on the school district system may not be encrypted without the permission of appropriate school authorities.

8. Users will not use the school district system to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.

9. Users will not use the school district system for conducting business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement. Users will not use the school district system to purchase goods or services for personal use without authorization from the appropriate school district official.

10. Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district's Policy 514 Bullying Prohibition Policy. This prohibition includes using any technology or other electronic communication off school premises to the extent that student learning or the school environment is substantially and materially disrupted.

B. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school district premises also may be in violation of this policy as well as other school district policies. Examples of such violations include, but are not limited to, situations where the school district system is compromised or if a school district employee or student is negatively impacted. If the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school district may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to the school district computer system and the Internet and discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment.

C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. In the case of a school district employee, the immediate disclosure shall be to the employee's immediate

supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.

~~V. INTERNET/INTRANET CONTENT AND STUDENT SAFTEY~~

~~The Internet is not under the control of this school district, and making Internet available to students carries with it the possibility that some students might encounter information that may be controversial or inappropriate for students. ISD 726 denies any responsibility for the accuracy or quality of the information obtained.~~

~~ISD 726 will employ technology protection systems in compliance with federal legislation, and Internet content is monitored with technology tools to limit access to material that is sexually explicit, prurient or obscene. While diligent effort will be made to block access to sites with such content, the constantly changing nature of the Internet prevents any technology filtering system from blocking all inappropriate material.~~

~~At the request of a classroom teacher, the media/technology personnel may adjust the settings of the software filter temporarily to accommodate a particular lesson that might require students to access materials otherwise blocked. If the unblocked material is deemed sexually explicit, prurient or obscene, parent notification would occur.~~

~~Ultimately parents and guardians are expected to set and communicate the standards that their children should follow when using this resource. To that end, the Becker School District will support each family's right to restrict their child from accessing the Internet by submitting that request in writing to the building administrator.~~

VI. ~~WEB PUBLICATION AND STUDENT DATA PRIVACY~~ FILTER

~~In accordance with Policy 515 Protection And Privacy Of Pupil Records, some student directory information, such as a student's name or photograph, may be posted on the district website, so far as the information is not personally identifiable. The District shall annually give public notice to inform parents of the types of student information the district has designated as directory information and of the parent's right to refuse to let the school district designate any or all of those types of information about the student pursuant to the aforementioned policy.~~

A. With respect to any of its computers or devices with Internet access, the school district will monitor the online activities of both minors and adults and employ technology protection measures during any use of such

computers by minors and adults. The technology protection measures utilized will 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, an actual or simulated sexual act or sexual contact, 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.

C. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint.

D. An administrator, supervisor, or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

E. The school district will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the school district computer system and use of the Internet shall be consistent with school district policies and the mission of the school district.

VIII. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the school district system.

B. ~~Users must keep all account information and passwords on file with the designated school district official.~~ Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law.

C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.

D. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents have the right to request the termination of a child's individual account at any time.

E. ~~The school district retains the right at any time to investigate or review the contents of all files, including email files.~~ School district employees should be aware that ~~data and other materials in files maintained on~~ the school district retains the right at any time to investigate or ~~server may be subject to~~ review the contents of their files and e-mail files. In addition, school district employees should be aware that data and other materials in files maintained on the school district system may be subject to review, disclosure or discovery under Minn Stat Ch. 13 (Minnesota Government Data Practices Act).

F. 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.

IX. INTERNET USE AGREEMENT

A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents, and employees of the school district.

B. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.

C. The Internet Use Agreement form for students must be read and signed by the user, the parent or guardian, and the supervising teacher. The Internet Use Agreement form for employees must be signed by the employee. The form must then be filed at the school office. As supervising teachers change, the agreement signed by the new teacher shall be attached to the original agreement.

~~VIII~~X. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district system is at the user's own risk. The system is provided on an "as is, as available" basis. The 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 diskettes, tapes, hard drives, or servers ~~or media~~, or for delays, or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

XI. USER NOTIFICATION

A. All users shall be notified of the school district policies relating to Internet use.

B. This notification shall include the following:

1. Notification that Internet use is subject to compliance with school district policies.

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

a. Information stored on school district diskettes, hard drives, or servers.

b. Information retrieved through school district computers, networks, or online resources.

c. Personal property used to access school district computers, networks, or online resources.

d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.

3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.

4. Notification that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial

obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents.

6. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records.

7. Notification that, should the user violate the school district's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.

8. Notification that all provisions of the acceptable use policy are subordinate to local, state, and federal laws.

XII. PARENTS' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

A. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media. Parents are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.

B. Parents will be notified that their students will be using school district resources/accounts to access the Internet and that the school district will provide parents the option to request alternative activities not requiring Internet access. This notification should include:

1. A copy of the user notification form provided to the student user.

2. A description of parent/guardian responsibilities.

3. A notification that the parents have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.

4. A statement that the Internet Use Agreement must be signed by the user, the parent or guardian, and the supervising teacher prior to use by the student.

5. A statement that the school district's acceptable use policy is

available for parental review.

XIII. IMPLEMENTATION; POLICY REVIEW

A. The school district administration may develop appropriate user notification forms, guidelines, and procedures necessary to implement this policy.

B. The administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The school district Internet policies and procedures are available for review by all parents, guardians, staff, and members of the community.

Legal References: 15 U.S.C. § 6501 *et seq.* (Children's Online Privacy Protection Act)
17 U.S.C. § 101 *et seq.* (Copyrights)
20 U.S.C. § 6751 *et seq.* (Enhancing Education through Technology Act of 2001)
47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA))
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Minn. Stat. § 121A.031 (School Student Bullying Policy)
Minn. Stat. § 125B.15 (Internet Access for Students)
Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 89 S.Ct. 733, 21 L.Ed.2d 731 (1969)
United States v. Amer. Library Assoc., 539 U.S. 194, 123 S.Ct. 2297, 56 L.Ed.2d 221 (2003)
Doninger v. Niehoff, 527 F.3d 41 (2nd Cir. 2008)
R.S. v. Minnewaska Area Sch. Dist. No. 2149, No. 12-588, 2012 WL 3870868 (D. Minn. 2012)
Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011), aff'd on other grounds 816 N.W.2d 509 (Minn. 2012)
S.J.W. v. Lee's Summit R-7 Sch. Dist., 696 F.3d 771 (8th Cir. 2012)
Kowalski v. Berkeley County Sch., 652 F.3d 656 (4th Cir. 2011)
Layshock v. Hermitage Sch. Dist., 650 F.3d 205 (3rd Cir. 2011)
Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch. Dist., 853 F.Supp.2d 888 (W.D. Mo. 2012)
M.T. v. Cent. York Sch. Dist., 937 A.2d 538 (Pa. Commw. Ct. 2007)
J.S. v. Bethlehem Area Sch. Dist., 807 A.2d 847 (Pa. 2002)

Cross References: Policy 406 (Public and Private Personnel Data)

Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
Policy 506 (Student Discipline)
Policy 514 (Bullying Prohibition Policy)
Policy 515 (Protection and Privacy of Pupil Records)
Policy 519 (Interviews of Students by Outside Agencies)
Policy 521 (Student Disability Nondiscrimination)
Policy 522 (Student Sex Nondiscrimination)
Policy 603 (Curriculum Development)
Policy 604 (Instructional Curriculum)
Policy 606 (Textbooks and Instructional Materials)
Policy 806 (Crisis Management Policy)
Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)