

Adopted: 3/97

Burnsville-Eagan-Savage School District Policy 524

Reviewed: 4/12/2018

Revised: 4/26/2018 MSBA 2018 NS

Rescinds: IIBG and IIBG-E

524 INTERNET ACCEPTABLE USE AND SAFETY POLICY

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the school district computer system and acceptable and safe use of the Internet and other digital resources. This policy also applies to the use of personally owned computing devices when used in school and on school networks and on non-school networks during school.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the school district digital resources the school district considers its own stated educational mission, goals, and objectives. Digital literacy skills are now fundamental to preparation of citizens and future employees. Access to the school district digital resources enables students and employees to explore thousands of libraries, databases, expert opinions, and other resources while exchanging messages with people around the world. The school district expects that faculty will blend thoughtful use of digital resources, student-owned communication devices, and the Internet throughout the curriculum and will provide guidance and instruction to students in their use as part of the mandated curriculum. Students will recognize that responsibility for positive uses of digital resources belongs to them.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school's digital resources which includes Internet access. The purpose of the resources 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 resources for classroom activities, educational research, and professional or career development activities. Users are expected to use Internet access and other digital resources 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.

IV. USE OF DIGITAL RESOURCES

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.

V. UNACCEPTABLE USES

- A. The following uses of the school district digital resources are considered unacceptable:
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.
 - f. Users will not use external proxy servers or other means of bypassing the district's Internet content filter to gain access to these materials.
 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 digital resources 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 digital resources 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 guardians 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 or 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. The district may set up user accounts for students in commercial products in which the user agreement follows COPPA compliance.

Vetting of such products is to be done at the district level.

7. Users must keep all account information and passwords on file with the designated school district official. 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 digital resources 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 non-licensed software or media or copying software or media to or from any school computer. Users will give proper attribution to works in all media they find on the Internet.
 9. Users will not use the school digital resources 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.
 10. Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district's Bullying Prohibition Policy 514. 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.

- D. Students and employees using privately-owned electronic devices must follow the policy stated in this document while on school property, attending any school-sponsored activity, or using the [school] network.

VI. FILTER

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

The term “harmful to minors” means any picture, image, graphic image file, or other visual depiction that:

- a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
 - b. 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
 - c. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
 - d. Can be considered hate speech (as defined by law).
 - e. Can be considered a recruiting tool for radical organizations (as defined by law).
- B. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint.
 - C. 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.

- D. 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.
- E. The school district may create filtering policies specific to groups using defined processes.

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. 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 only if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.
- D. School district employees should be aware that the school district retains the right at any time to investigate or 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 (the Minnesota Government Data Practices Act).

IX. DIGITAL RESOURCES USE AGREEMENT

- A. The proper use of digital resources including the Internet, and the educational value to be gained from proper digital resource use, is the joint responsibility of students, parents or guardians, 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. Annually, a building administrator, principal or designated staff member is responsible to inform students of policies and guidelines for access to the school

district computer system and acceptable and safe use of the internet, including all electronic communications.

X. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district digital resources is at the user's own risk. The system is 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 any media or contracted service, including but not limited to, hard drives, servers, or cloud-based applications 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, servers, or officially contracted vendor applications.
 - 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 or guardians.

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 OR GUARDIANS' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

- A. Outside of school, parents or guardians 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 or guardians 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 or guardians will be notified that their students will be using school district resources/accounts to access the Internet. 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 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 for submission to the school board for approval. Upon approval by the school board, such guidelines, forms, and procedures shall be an addendum to 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.

- D. Because of the rapid changes in the development of the Internet, the school board shall conduct an annual review of this policy.

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.0695 (School Board Policy; Prohibiting Intimidation and Bullying)
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: Burnsville-Eagan-Savage School District Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
Burnsville-Eagan-Savage School District Policy 406 (Public and Private Personnel Data)
Burnsville-Eagan-Savage School District Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
Burnsville-Eagan-Savage School District Policy 506 (Student Discipline)
Burnsville-Eagan-Savage School District Policy 514 (Bullying Prohibition Policy)
Burnsville-Eagan-Savage School District Policy 515 (Protection and Privacy of Pupil Records)
Burnsville-Eagan-Savage School District Policy 519 (Interviews of Students by Outside Agencies)
Burnsville-Eagan-Savage School District Policy 521 (Student Disability)

Nondiscrimination)
Burnsville-Eagan-Savage School District Policy 522 (Student Sex
Nondiscrimination)
Burnsville-Eagan-Savage School District Policy 603 (Curriculum
Development)
Burnsville-Eagan-Savage School District Policy 604 (Instructional
Curriculum)
Burnsville-Eagan-Savage School District Policy 606 (Textbooks and
Instructional Materials)
Burnsville-Eagan-Savage School District Policy 806 (Emergency
Operations Policy)
Burnsville-Eagan-Savage School District Policy 904 (Distribution of
Materials on School District Property by Nonschool Persons)