

Adopted: 9/23/2021

Burnsville-Eagan-Savage School District Policy 634

Reviewed: ~~02/27/2025~~ PRC 6/17/25

Revised: 03/13/2025

Rescinds: IIBG and IIBG-E, 524

634 INTERNET, ~~AND~~ TECHNOLOGY, ~~AND CELL PHONE~~ 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, including electronic communications.

II. GENERAL STATEMENT OF POLICY

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. 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 EDUCATION PURPOSE

The school district is providing students and employees with access to the school district computer system, which includes Internet access. 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.

IV. DEFINITIONS

- A. The term "Electronic Technologies" includes, but is not limited to, computer hardware and software, operating systems, web-based information and applications, telephones and other telecommunications equipment, video and multimedia equipment, information kiosks, and office products such as copiers and printers.
- B. The term "District Network" includes any equipment or interconnected system or

subsystem that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, transmission, or reception of data or information. The District Network is inclusive of all infrastructure necessary to provide and manage systems including but not limited to internet access, data, telecommunications, and wifi.

- C. The term “user” refers to any person using the District’s electronic technologies or network.

V. USE OF SYSTEM IS A PRIVILEGE

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.

VI. SECURITY

- A. The District has a cybersecurity program which maintains appropriate levels of access to District information and resources. Security practices apply to all users and for all District operations and activities. Unauthorized access, use, transfer, distribution, compromise or change of District data by any employee, student, or any other individual, may result in disciplinary action, which may include a recommendation for termination and other legal action. In order to effectively implement this policy, the District will:
 - 1. Implement standards and procedures to effectively manage and provide necessary access to District data, while at the same time ensuring, to the extent possible, the confidentiality, integrity, and security.
 - 2. Maintain an information security program based on risk assessment that follows relevant best practices in the field of information security.
 - 3. Provide processes for evaluating and vetting software that interfaces with District data, including processes for evaluating third parties and their security practices.

VII. UNACCEPTABLE USES

- A. While not an exhaustive list, the following uses of the school district system and Internet resources or accounts 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.
- 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 engage in political campaigning.
 - 5. 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.
 - 6. Users will not use external proxy servers or other means of bypassing the district's internet content filter or security measures.
 - 7. 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.
 - 8. 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 “Facebook,” “Twitter,” “Instagram,” “Snapchat,” “TikTok,” “Reddit,” and similar websites or applications.

- 9. 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.
- 10. 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.

11. 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.
 12. Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district's 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. The school district has a special interest in regulating off-campus speech that materially disrupts classwork or involves substantial disorder or invasion of the rights of others. 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 may include, but are not limited to, serious or severe bullying or harassment targeting particular individuals, threats aimed at teachers or other students, failure to follow rules concerning lessons, the writing of papers, the use of computers, or participation in other online school activities, and breaches of school security devices. 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. The District does not support personal equipment. Users will not attach any personal equipment or install software on any District-owned systems. Users may use personal devices on the District's guest WIFI.

VIII. FILTER

- A. With respect to any of its computers 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 use best efforts and industry standard approaches 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, 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. Access to chat rooms, discussion boards, school-issued email and other forms of direct electronic communications are limited to applications approved by the District and/or hosted within the District domain for the safety and security of minors. Access to communication tools may be adjusted based on student age.
- D. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint.
- E. 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.
- F. The District is obligated to monitor and/or review filtering activities.
- G. 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.

IX. 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.

X. 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 if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.
- D. Parents may have the right at any time to investigate or review the contents of their child's files and e-mail files in accordance with the school district's Protection and Privacy of Pupil Records Policy.
- E. 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 Minnesota Statutes chapter 13 (Minnesota Government Data Practices Act).
- F. It is recommended that electronic mail contain a confidentiality notice, similar to the following:

If the information in this email is related to an individual or student, it may be private data under state or federal privacy law. This individual private data should not be reviewed, distributed or copied by any person other than the intended recipient(s), unless otherwise permitted under law. If you are not the intended recipient, any further review, dissemination, distribution, or copying of this electronic communication or any attachment is strictly prohibited. If you have received an electronic communication in error, you should immediately delete it from your system.
- G. 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.

XI. 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. By using the district's internet and technology resources, users accept the terms of this policy.

XII. 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 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 diskettes, tapes, hard drives, or servers, 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.

XIII. 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 of password ownership and password protection procedures.
5. 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.
6. 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.
7. Notification that student email addresses may be provided to District-approved third-party providers for access to educational tools and content.
8. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by Public and Private Personnel Data Policy, and Protection and Privacy of Pupil Records Policy.
9. 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.
10. Notification that all provisions of the acceptable use policy are subordinate to local, state, and federal laws.

XIV. 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.

XV. NOTIFICATION REGARDING TECHNOLOGY PROVIDERS

- A. "Technology provider" means a person who:
 1. contracts with the school district, as part of a one-to-one program or otherwise, to provide a school-issued device for student use; and

2. creates, receives, or maintains educational data pursuant or incidental to a contract with the school district.
- B. “Parent” means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian.
- C. Within 30 days of the start of each school year, the school district must give parents and students direct and timely notice, by United States mail, e-mail, or other direct form of communication, of any curriculum, testing, or assessment technology provider contract affecting a student’s educational data. The notice must:
 1. identify each curriculum, testing, or assessment technology provider with access to educational data;
 2. identify the educational data affected by the curriculum, testing, or assessment technology provider contract; and
 3. include information about the contract inspection and provide contact information for a school department to which a parent or student may direct questions or concerns regarding any program or activity that allows a curriculum, testing, or assessment technology provider to access a student’s educational data.
- D. The school district must provide parents and students an opportunity to inspect a complete copy of any contract with a technology provider.
- E. A contract between a technology provider and the school district must include requirements to ensure appropriate security safeguards for educational data. The contract must require that:
 1. the technology provider’s employees or contractors have access to educational data only if authorized; and
 2. the technology provider’s employees or contractors may be authorized to access educational data only if access is necessary to fulfill the official duties of the employee or contractor.
- F. All educational data created, received, maintained, or disseminated by a technology provider pursuant or incidental to a contract with a public educational agency or institution are not the technology provider’s property.

XVI. SCHOOL-ISSUED DEVICES

- A. “School-issued device” means hardware or software that the school district, acting independently or with a technology provider, provides to an individual student for that student’s dedicated personal use. A school-issued device includes a device issued through a one-to-one program.

- B. Except as provided in paragraph C, the school district or a technology provider must not electronically access or monitor:
 - 1. any location-tracking feature of a school-issued device;
 - 2. any audio or visual receiving, transmitting, or recording feature of a school-issued device; or
 - 3. student interactions with a school-issued device, including but not limited to keystrokes and web-browsing activity.
- C. The school district or a technology provider may only engage in activities prohibited by paragraph B if:
 - 1. the activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by school district employees, student teachers, staff contracted by the school district, a vendor, or the Minnesota Department of Education, and notice is provided in advance;
 - 2. the activity is permitted under a judicial warrant;
 - 3. the school district is notified or becomes aware that the device is missing or stolen;
 - 4. the activity is necessary to respond to an imminent threat to life or safety and the access is limited to that purpose;
 - 5. the activity is necessary to comply with federal or state law, including but not limited to Minnesota Statutes section 121A.031; or
 - 6. the activity is necessary to participate in federal or state funding programs, including but not limited to the E-Rate program.
- D. If the school district or a technology provider interacts with a school-issued device as provided in paragraph C, clause 4, it must, within 72 hours of the access, notify the student to whom the school-issued device was issued or that student's parent and provide a written description of the interaction, including which features of the device were accessed and a description of the threat. This notice is not required at any time when the notice itself would pose an imminent threat to life or safety, but must instead be given within 72 hours after that imminent threat has ceased.

XVII. PERSONAL DEVICE ACCESS

- A. Personal Devices may be used only on the district's guest WIFI and must abide by the district's Acceptable Use Policy.
- B. Personal devices may not be connected to other networks besides public WIFI and may not be connected to any district equipment.

C. Though guests may use their personal devices and expect some aspects of privacy, use of our network and systems have the following expectations:

1. **Use at your own risk.** Use of the Burnsville-Eagan-Savage District 191 network is at the device owner's discretion and therefore Burnsville Public Schools is not responsible for any loss, damage or adverse effects that may occur to a device while on our network.
2. **The District 191 network is filtered.** Known inappropriate and/or malicious sites, and many non-instructional sites, are blocked. Use of the district network and systems requires that owners of personal devices adhere to legal and ethical conduct, and refrain from attempting to access blocked content.
3. **Expectation of privacy.** Access to the contents of a personal devices is governed by local and federal laws. However, while accessing The District 191 network, systems and buildings, there is not a right to privacy of any content, and as such, may be monitored for inappropriate or illegal activities.
4. **District 191 reserves the right to maintain records of usage.** Burnsville-Eagan-Savage District 191 immediately terminates the privilege to use its network should it become aware that the network is being used for inappropriate or illegal activities. The district reserves the right to take appropriate action in the event inappropriate or illegal activities are discovered on our systems or network.

XVIII. CELL PHONE USE

~~———— The school board directs the superintendent and school district administration to establish rules and procedures regarding student possession and use of cell phones in schools. These rules and procedures should seek to minimize the negative impact of cell phones on student behavior, mental health, and academic attainment. These rules and procedures may be designed for grades K-5, 6-8, 9-12 and special programs.~~

~~———— If the school district has a reasonable suspicion that a student has violated a school policy, rule, or law by use of a cell phone or other electronic communication device, the school district may search the device. The search of the device will be reasonably related in scope to the circumstances justifying the search.~~

~~———— Students who use an electronic communication device during the school day and/or in violation of school district policies may be subject to disciplinary action pursuant to the school district's discipline policy. In addition, a student's cell phone or electronic communication device may be confiscated by the school district and, if applicable, provided to law enforcement. Cell phones or other electronic communication devices that are confiscated and retained by the school district will be returned in accordance with school building procedures.~~

XVIII. LIMIT ON SCREEN TIME FOR CHILDREN IN PRESCHOOL AND KINDERGARTEN

A child in a publicly funded preschool or kindergarten program may not use an individual-use screen, such as a tablet, smartphone, or other digital media, without engagement from a teacher or other students. This section does not apply to a child for whom the school has an individualized family service plan, an individualized education program, or a 504 plan in effect.

~~XIX~~. 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.

~~XXI~~. 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 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 diskettes, tapes, hard drives, or servers, 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.

Legal References: Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act)
Minn. Stat. § 13.32 (Educational Data)
Minn. Stat. § 121A.031 (School Student Bullying Policy)
Minn. Stat. § 121A.73 (School Cell Phone Policy)
Minn. Stat. § 124D.166 (Limit on Screen Time for Children in Preschool and Kindergarten)
Minn. Stat. § 125B. 15 (Internet Access for Students)
Minn. Stat § 125B.26 (Telecommunications/Internet Access Equity Act)
15 U.S.C § 6501 *et seq.* (Children's Online Privacy Protection Act)
17 U.S.C § 101 *et seq.* (Copyrights)

47 U.S.C § 254 (Children’s Internet Protection Act of 2000 (CIPA))
 20 U.S.C § 6751 et se. (Enhancing Education Through Technology Act of 2001)
 20 U.S.C. § 1232g (Family Educational Rights and Privacy Act)
 47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Mahanoy Area Sch. Dist. v. B.L., 594 U.S. 180, 141 S. Ct. 2038 (2021)
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969)
States v. American Library Association, 539 U.S. 194 (2003)
Sagehorn v. Indep. Sch. Dist. No. 728, 122 F.Supp.2d 842 (D. Minn. 2015)
R.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F.Supp.2d 1128 (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)
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)
Layshock v. Hermitage Sch. Dist., 650 F.3d 205 (3rd Cir. 2011)
JS 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 422 (Policies Incorporated by Reference)
 Burnsville-Eagan-Savage School District Policy 498 (Political Campaign & Activities)
 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 524 \(Personal Electronic Communication Devices Including Cell Phones\)](#)
 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 622 (Copyright Policy)
 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)

