634 ELECTRONIC TECHNOLOGIES ACCEPTABLE USE POLICY

I. PURPOSE

This policy sets forth parameters and guidelines for access to the school district's electronic technologies, use of personal electronic devices within the district, electronic communications, use of the district's network, internet, and social networking tools.

II. GENERAL STATEMENT OF POLICY

Technology is one of many learning tools. The use of technology needs to be safe, appropriate, and aligned with the mission of the district. Access to the district's computer network and internet enables students and employees to explore libraries, databases, web pages, other online resources, and connect with people around the world. The district expects its instructional staff to blend safe and thoughtful use of the district's computer network, educational technologies and the internet throughout the curriculum, providing guidance to students.

III. DEFINITIONS

A. Electronic Technologies include but are 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. Social Networking Tools are computer software and web-based services that enable people to interact with each other and include but are not limited to blogs, wikis, video conferencing, online chat, and instant messaging.

C. The District Network is 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.

D. The term "harmful to minors" means any that: materials 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.

IV. EDUCATIONAL USES

Use of the district's electronic technologies is for educational purposes and district operations only. Use of district electronic resources is limited to district employees, students, or other guests with expressed permission. Students and employees are expected to use electronic technologies to further the district's educational mission, goals and strategic direction. Students and employees are expected to use the district's electronic technologies to support classroom activities, educational research or professional enrichment.

Use of the district's electronic technologies is a privilege, not a right. The district's network, an educational technology, is a limited forum; the district may restrict speech for educational reasons.

V. GUIDELINES IN USE OF ELECTRONIC TECHNOLOGIES

A. Electronic technologies are assets of the school district and are protected from unauthorized access, modification, destruction or disclosure. Use of personal devices, while on district property, is subject to all policies and guidelines, as applicable, plus any state and federal laws related to internet use, including copyright laws.

B. The district reserves the right to monitor, read or copy any item on or using the district's electronic technologies, including its network.

C. Students and employees will not vandalize, damage or disable any electronic technology or system used by the district.

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

E. Routine maintenance and monitoring of electronic technologies, including the district network, may lead to a discovery that a user has violated this policy, another school district policy or the law.

VI. UNACCEPTABLE USES OF ELECTRONIC TECHNOLOGIES AND DISTRICT NETWORK

Misuse of the district's electronic technologies may lead to discipline of the offending employee or student. The following uses of school district electronic technologies while either on/off district property and/or personal electronic technologies while on district property and district network ("electronic technologies") are considered

unacceptable:

A. Users will not use electronic technologies to create, access, review, upload, download, complete, store, print, post, receive, link, transmit or distribute:

1. Pornographic, obscene or sexually explicit material or other visual depictions;

2. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or sexually explicit language;

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

4. Materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment, discrimination or threatens the safety of others;

5. Orders for shopping online during time designated as work time by the district; and

6. Storage of personal photos, videos, music or files not related to educational purposes for any length of time.

B. Users will not use electronic technologies 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.

C. Users will not use electronic technologies to engage in any illegal act or violate any local, state or federal laws.

D. Users will not use electronic technologies for political campaigning.

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

F. Users will not use electronic technologies 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.

G. Users must not deliberately or knowingly delete a student or employee record.

H. Users will not use electronic technologies to post information in public access areas regarding private or confidential information about another person. Private or confidential information is defined by board policy, state law, and federal law.

1. This paragraph does not prohibit the posting of employee contact information on district web pages. Refer to Policy 515 (Protection and Privacy of Student Records) for direction on directory information for students and how this can be used.

2. This paragraph does not prohibit communications between employees and other individuals when such communications are made for legitimate education reasons or personnel-related purposes (i.e. communications with parents or other staff members related to students).

3. This paragraph specifically prohibits the use of electronic technologies to post private or confidential information about another individual, employee or student, on social networks.

I. Users will not repost or resend a message that was sent to the user privately without the permission of the person who sent the message.

J. Users will not attempt to gain unauthorized access to the district's electronic technologies or any other system through electronic technologies, 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. Users must keep all account information and passwords private.

K. Users will not use external proxy servers or other means of bypassing the district's internet content filter.

L. Messages and records on the district's electronic technologies may not be encrypted without the permission of director of technology.

M. Users will not use electronic technologies to violate copyright laws or usage licensing agreements:

1. Users will not use another person's property without the person's prior approval or proper citation;

2. Users will not download, copy or exchange pirated software including freeware and shareware; and

3. Users will not plagiarize works found on the internet or other information resources.

N. Users will not use electronic technologies for unauthorized commercial purposes or financial gain unrelated to the district's mission. Users will not use electronic technologies to offer or provide goods or services or for product placement.

O. Use of Unmanned Airborne Vehicles (UAVs) or drones is prohibited on school property without prior approval of the director of technology, director of operations, properties and transportation or building principal.

VII. USER NOTIFICATION

Users will be notified of school district policies relating to internet use. This notification must include the following:

A. Notification that internet use is subject to compliance with district policies.

B. Disclaimers limiting the district's liability relative to:

1. Information stored on district disks, drives or servers.

2. Information retrieved through district computers, networks or online resources.

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

4. Unauthorized financial obligations resulting from use of district resources or accounts to access the internet.

C. A description of the privacy rights and limitations of district sponsored or managed internet accounts.

D. 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 Student Records.

E. Notification that should the user violate this policy, the user's access privileges may be revoked, academic sanctions may result, school disciplinary action may be taken, and/or appropriate legal action may be taken.

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

G. Family Notification

1. Notification that the district uses technical means to limit student internet access however, the limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

2. 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 or

the student's parents.

VIII. STUDENTS

A. Internet Use Agreement

1. The proper use of the internet and educational technologies and the educational value to be gained from proper usage is the joint responsibility of students, parents and employees of the school district.

2. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a district account or educational technologies to access the internet.

3. Students have access to internet resources.

4. Students using social networking tools and curriculum content management software for a teacher's assignment are required to keep personal information as stated above out of their postings (see Section VI.H).

5. Students using educational technologies for social networking are limited to educational purposes and must follow the Online Code of Ethics (Appendix I and Policy 514, Bullying Prohibition.

B. Parents' Responsibility; Notification of Student Internet Use

Outside of school, parents bear responsibility for the same guidance of internet use as they exercise with other technology information sources. Parents are responsible for monitoring their student's use of the district system and district educational technologies, even if the student is accessing the district system from home or a remote location.

IX. GUEST ACCESS AND INTERNET USE

A. Guest access to the school district's open wireless network is provided as a service to the community, and is subject to all district policies and guidelines, plus any state and federal laws related to internet use, including copyright laws. See Appendix lI, Personal Device Access.

B. Guest access provides limited bandwidth, filtered for the following services:

1. Web access
2. Email services
3. Virtual private network services (VPN)

Limited technical support is provided for guest access

X. EMPLOYEES

A. Use of Email

The school district provides access to electronic mail for district communication between district employees and students, families, and community.

1. All emails received by, sent through, or generated by computers using the district network are subject to review by the district.

2. All emails are assumed to be documents that can be disclosed to the public unless the content of the email is protected as private or confidential information under data privacy laws. All information contained in an email must be treated in accordance with Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Student Records, regarding student and employee data privacy.

3. Employees will not provide access to their email accounts to non- employees.

4. It is recommended that electronic mail contain a confidentiality notice, similar to the following:

   If the information in this email relates to an individual or student, it may be private data under state or federal privacy laws. 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 return it to the sender and delete it from your system.

5. Employees will report inappropriate emails to the employee's supervisor or the director of technology.

6. Emails having content governed by the district's record retention schedule must be kept in accordance with the retention schedule.

B. Use of Electronic Technologies

1. Electronic technologies are provided primarily for work-related, educational purposes.

2. Inappropriate use of electronic technologies includes, but is not limited to:

   a. Posting, viewing, downloading or otherwise receiving or transmitting offensive, defamatory, pornographic or sexually explicit materials;
   b. Posting, viewing, downloading or otherwise receiving or transmitting materials that use language or images that advocate violence or discrimination toward other persons;

   c. Posting, viewing, downloading or otherwise receiving or transmitting material that may constitute harassment or discrimination contrary to district policy and state and federal law;

   d. Engaging in computer hacking or other related activities;

e. Attempting to, actually disabling or compromising the security of information contained on the district network or any computer; and

f. Engaging in any illegal act in violation of any local, state or federal laws.

3. Employees may participate in public internet discussion groups using the electronic technologies, but only to the extent that the participation:

a. Is work-related;

b. Does not reflect adversely on the district;

c. Is consistent with district policy; and

d. Does not express any position that is, or may be interpreted as, inconsistent with the district's mission, goal or strategic plan.

4. Employees may not use the district network or electronic technologies to post unauthorized or inappropriate personal information about another individual on social networks.

5. Employees will observe all copyright laws. Information posted, viewed or downloaded from the internet may be protected by copyright. Employees may reproduce copyrighted materials only in accordance with Policy 622, Copyright Policy.

6. All files downloaded from the internet must be checked for possible computer viruses. The district authorized virus checking software installed on each district computer will ordinarily perform this check automatically; however, employees should contact the district's director of technology before downloading any materials for which the employee has questions.

C. Employee Responsibilities

1. Employees who are transferring positions or leaving positions must leave all work-related files and electronic technologies, including form letters, handbooks, databases, procedures, and manuals, regardless of authorship, for their replacements.

2. Individual passwords for computers are confidential and must not be shared.

a. If an employee's password is learned by another employee, the password should be changed immediately.

b. An employee is responsible for all activity performed using the employee's password.

c. No employee should attempt to gain access to another employee's documents without prior express authorization.

d. An active terminal with access to private data must not be left unattended and must be protected by password protected screen savers.

3. Employees are expected to use technology necessary to perform the duties of their position.

4. Employees who fail to adhere to district policy are subject to disciplinary action in accordance with their collective bargaining agreement or contract. Disciplinary action may include suspension or withdrawal of internet or email access, payment for damages or repair, termination and/or referral to civil or criminal authorities for prosecution.

XI. DISTRICT WEB PRESENCE

The school district website provides information and a venue for communications with students, employees, parents and the community.

A. District Website

1. The district will establish and maintain a website. The website will include information regarding the district, its schools, district curriculum, extracurricular activities and community education.

2. The district webmaster will be responsible for maintaining the district website and monitoring district web activity.

3. All website content will support and promote the district's mission, goals and strategic direction.

4. The district's website will provide parents with a web portal to resources.

B. School Website

1. Each school will establish and maintain a website. The website will include information regarding the school, its employees, and activities.

2. The principal will appoint staff, who will be responsible for maintaining the school's website.

3. All website content will support and promote the district's mission, goals and strategic direction.

C. Classroom and Teacher Online Content

1. Teachers have the option of establishing a website that supports classroom instruction. The district may provide a standard option within the district's website for basic information about the teacher, such as contact information, personal narrative and links to class resources.
2. If a teacher establishes a web page, they are responsible for maintaining the web page.

3. Teacher web pages must be linked to the teacher's staff directory page.

D. Student Online Content

1. Students may create online content as part of classroom activities with teacher supervision.

2. Student online content must follow the Online Code of Ethics, Appendix I.

3. The classroom teacher will monitor all student-produced online content produced as part of classroom assignments and remove inappropriate material.

4. A classroom teacher or advisor will review student-produced online content to determine if the contents should be removed at the conclusion of the course grading period or activity.

E. Department and Noninstructional Online Content

1. Departments and noninstructional programs may also create online content, including web pages to support their departments or programs.

2. The establishment of web pages must be approved by the program administrator.

3. Once established, the individual departments or programs must appoint an employee(s) who will maintain the web page.

F. District Activity Online Content

1. With the approval of the building principal, a school board-approved district activity may establish a web page.

2. All online content will support the activity and the district's mission, goals and strategic direction.

3. The building principal and his/her designee will oversee the content of these web pages.

XII. RECORDS MANAGEMENT AND ARCHIVING

All technological data is data under the Minnesota Government Data Practices Act, the Family Educational Rights and Privacy Act, Records Retention Schedule, and school board policy.

XIII. FILTER

A. With respect to any of its electronic technologies with internet access, and personal devices accessing the school district network, the district will follow the guidelines provided by the Children's Internet Protection Act, and will monitor the online activities of users and employ technology protection measures during any use of such electronic

technologies by users. The technology protection measures utilized will, to the extent possible, block or filter internet access to any material that is:

1. Obscene;

2. Child pornography; or

3. Harmful to minors.

XIV. LIABILITY

Use of the school district's educational technologies 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. The district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system, nor is it responsible for damages or injuries from improper communications or damage to property used to access school computers and online resources. The district will not be responsible for financial obligations arising through unauthorized use of the district's educational technologies or the internet.

XV. 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 information. These guidelines, forms and procedures will be an addendum to this policy.

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

C. The district electronic technologies policy is available for review by parents, employees and members of the community.

D. Due to the rapid evolution in educational technologies, the school board will 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)
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 (1969) *United States v. American Library Association*, 539 U.S. 194 (2003)

Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011)
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 Dist4rict Policy 422 (Policies Incorporated by Reference)
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)
Burnsville-Eagan-Savage School District Policy 515 (Protection and Privacy of Student Records)
Burnsville-Eagan-Savage School District Policy 521 (Student Disability Nondiscrimination)
Burnsville-Eagan-Savage School District Policy 603 (Curriculum Development)
Burnsville-Eagan-Savage School District Policy 606 (Instructional Resources)
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 Non-school Persons)

Appendix I to Policy 634

ONLINE CODE OF ETHICS

In Burnsville-Eagan-Savage School District 191, it is important to use information and technology in safe, legal, and responsible ways. At the same time, the district has a desire for our students to leave our system with a "positive digital footprint," so that employers and postsecondary institutions can see the great work that they have done. We embrace these conditions as facets of being a digital citizen and strive to help students develop a positive digital footprint.

1. Students accessing or using electronic products including but not limited to blogs, wikis, podcasts, Google applications and district learning management systems for student assignments are required to keep personal information out of their postings.

   At the high school level parents may opt to allow their students to utilize their full name in order to increase their positive digital footprint when publishing to an authentic audience.

2. Students will select online names that are appropriate and will consider the information and images that are posted online at an age appropriate level.

3. Students will not log in to the network as another classmate.

4. Students using electronic tools will treat these tools as a classroom space. Speech that is inappropriate for class is not appropriate on electronic tools. Students are expected to treat others and their ideas online with respect.

5. Assignments on electronic tools are like any other assignment in school. Students, in the course of completing the assignment, are expected to abide by policies and procedures in the student handbook, including those policies regarding plagiarism and acceptable use of technology.

6. Electronic forums for student expression; are first and foremost tools for learning. The district may restrict speech for valid educational reasons as outlined in board policy.

7. Students will not use the internet, in connection with the teacher assignments, to harass, discriminate, bully or threaten the safety of others. If students receive a comment on an electronic forum used in school that makes them feel uncomfortable or is not respectful, they must report this to a teacher, and must not respond to the comment. Student conduct that occurs off-campus, but has a connection to the school environment, may form the basis for school discipline. This specifically includes activities that occur off campus over the internet, on social media, or through other communications.

8. Students accessing electronic tools from home or school, using school equipment, will not download or install any software without permission.

9. Students should be honest, fair and courageous in gathering, interpreting and expressing information for the benefit of others. Always identify sources and test the accuracy of information from all sources.

10. Students will treat information, sources, subjects, colleagues and information consumers as people deserving of respect. Gathering and expressing information should never cause harm or threaten to be harmful to any person or group of people.

11. Students are accountable to their readers, listeners and viewers and to each other. Admit mistakes

and correct them promptly. Expose unethical information and practices of others.

12. Users will not repost or resend content that was sent to the user privately without the permission of the person who created the content.

13. School board policies concerning acceptable use of electronic technology include the use of these electronic tools for school activities (Policy 634: Electronic Technologies Acceptable Use Policy).

14. Failure to follow this code of ethics will result in academic sanctions and/or disciplinary action.

Revised: Modified:

Appendix ll to Policy 634

Personal Device Access

Users of personal devices connecting to the Burnsville-Eagan-Savage School District 191 public network must abide by district's Electronic Technologies Acceptable Use Policy (Board Policy 634).
Though guests may use their personal device 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 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. 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.