Adopted: 9/23/2021
Reviewed: ~~11/9/2023~~ PRC 02/18/25
Revised: 11/17/2022
Rescinds: IIBG and IIBG-E, 524

634 ~~ELECTRONIC TECHNOLOGIES~~ INTERNET, 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.~~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

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.
~~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. 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. ~~A.~~ The term "Electronic Technologies" includes, but ~~are~~ 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. 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.~~

B~~C~~. The term "District Network" includes ~~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.

C. The term "user" refers to any person using the District's electronic technologies or network.

~~D. The term "harmful to minors" means any 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.~~

V. USE OF SYSTEM IS A PRIVLEGE

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 if 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 provides 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. ~~specific school buildings, grade levels, or similar criteria.~~

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.

XIX. 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.

XX. 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.

~~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 II, 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 their 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.

XII. 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~~ XXI. LIABILITY

Use of the school district~~'s~~ system ~~educational technologies~~ 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~~., nor is it responsible for damages or injuries from improper communications or damage to property used to access school computers and online resources~~. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system ~~'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: 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 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)

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.