

Adopted: 09/18/97

Independent School District# 118 Policy 524

Annual Review: 3/15/07,03/09, 11/21/12,

Revised: 04/20/00, 05/20/04 04/20/06, 12/2006, 3/15/07,02/08, 3/09

05/17/2012, 6/21/2012, 10/22/13, 01/06/14, 7/15/14, 2/18/16, 10/27/16, 1/3/18, 10/12/21, 8/22, 7/23

524 INTERNET ACCEPTABLE USE AND SAFETY POLICY

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the school district computer system and acceptable and safe use of the Internet, including electronic communications.

II. GENERAL STATEMENT OF POLICY

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

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school district computer system, which includes Internet access. 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. USE OF SYSTEM IS A PRIVILEGE

The use of the school district system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate school

district policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

V. 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. Users will not use the school district system to engage in cyber bullying or harassment of another person, or to engage in personal attacks, including prejudicial or discriminatory attacks. This includes, but is not limited to, social network sites, tweeting, texting, chat rooms, email, and other electronic communications.
3. Users will not use the school district system to engage in any illegal act or violate any local, state, or federal statute or law.
4. Users will not use the school district system to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the school district system software, hardware or wiring or take any action to violate the school district's security system, and will not use the school district system in such a way as to disrupt the use of the system by other users.

5. Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information, or files without the implied or direct permission of that person.
6. Users will not use the school district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

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

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

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

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

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

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

social networks such as “Facebook,” “Twitter,” Instagram,” “Snapchat, and “Reddit” and similar websites of applications.

7. Users must keep all account information and passwords on file with the designated school district official. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district system, attempt to log in through another person’s account, or use computer accounts, access codes, or network identification other than those assigned to the user. Messages and records on the school district system may not be encrypted without the permission of appropriate school authorities.
 8. Users will not use the school district system to violate copyright laws or usage licensing agreements, or otherwise to use another person’s property without the person’s prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.
 9. Users will not use the school district system for conducting business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement. Users will not use the school district system to purchase goods or services for personal use without authorization from the appropriate school district official.
 10. Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district’s Bullying Prohibition Policy (MSBA/MASA Model Policy 514). This prohibition includes using any technology or other electronic communication off school premises to the extent that student learning or the school environment is substantially and materially disrupted.
- B. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school district premises also may be in violation of this policy as well as other school district policies. Examples of such violations include, but are not limited to, situations where the school district system is compromised or if a school district employee or student is negatively impacted. If the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school district may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to the school district computer system and the Internet and discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment.

- C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. In the case of a school district employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.
- 10. Users will not conduct personal business on district owned computers during the established workday.

Staff members will not use district owned computers for recreational use during established work hours.
- 11. Students must not be permitted to play non-educational games. Routinely allowing students to play games is strictly prohibited. However, it is permissible to allow a class and/or student as a reinforcer to use educationally related programs or sites.

VI. 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 block or filter Internet access to any visual depictions that are:
 - 1. Obscene;
 - 2. Child pornography; or
 - 3. Harmful to minors.
- B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
 - 1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
 - 2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

- 3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
- C. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint.
- D. An administrator, supervisor, or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.
- E. The school district will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response. Students will be taught about the benefit/hazards of online social behavior, social networking, and cyber bullying.

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES

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

VIII. LIMITED EXPECTATION OF PRIVACY

- A. By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the school district system.
- B. Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law.
- C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.
- D. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents have the right to request the termination of their child's individual account at any time.
- 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 (the Minnesota Government Data Practices Act).

- F. The school district will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.

IX. INTERNET USE AGREEMENT

- A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents, and employees of the school district.
- B. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet. Education on social networks, cyber bullying will be integrated into all computer classes.
- C. The Internet Use Agreement form for students must be read, approved, and signed by the user and the parent or guardian. The Internet Use Agreement form for employees must be signed by the employee. The form must then be filed at the school office. As supervising teachers change, the agreement signed by the new teacher shall be attached to the original agreement.

X. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district system is at the user's own risk. The system is provided on an "as is, as available" basis. The 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 misedeliveries or nondeliveries of information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

XI. USER NOTIFICATION

- A. All users shall be notified of the school district policies relating to Internet use.
- B. This notification shall include the following:
 - 1. Notification that Internet use is subject to compliance with school district policies.
 - 2. Disclaimers limiting the school district's liability relative to:
 - a. Information stored on school district diskettes, hard drives, or servers.

- b. Information retrieved through school district computers, networks, or online resources.
 - c. Personal property used to access school district computers, networks or online resources.
 - d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.
3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.
 4. Notification that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.
 5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents.
 6. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records.
 7. Notification that, should the user violate the school district's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.
 8. Notification that all provisions of the acceptable use policy are subordinate to local, state, and federal laws.

XII. PARENTS' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

- A. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media. Parents are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.
- B. Parents will be notified that their students will be using school district resources/accounts to access the Internet and that the school district will provide parents the option to request alternative activities not requiring Internet access. This notification should include:

1. A copy of the user notification form provided to the student user.
2. A description of parent/guardian responsibilities.
3. A notification that the parents have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.
4. A statement that the Internet Use Agreement must be signed by the user, the parent or guardian, and the supervising teacher prior to use by the student.
5. A statement that the school district's acceptable use policy is available for parental review.

XIII. 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.

XIV. 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.

XV. CELL PHONE USE

1. Students are prohibited from using cell phones and other electronic communication devices during the instructional day. Students also are prohibited from using a cell phone or other electronic communication device to engage in conduct prohibited by school district policies including, but not limited to, cheating, bullying, harassment, and malicious and sadistic conduct.
2. 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.
3. 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.

[Note: This language aligns with the provisions found in the MSBA Model Student Handbook. As an alternative to stating specific cell phone rules in a school district policy, a school board could choose to direct school administration to establish cell phone rules. This approach enables administrators to craft flexible and specific rules that are specific to grade levels and buildings.]

XVI. 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.

XVII. IMPLEMENTATION; POLICY REVIEW

- A. The school district administration may develop appropriate user notification forms, guidelines, and procedures necessary to implement this policy for submission to the school board for approval. Upon approval by the school board, such guidelines, forms, and procedures shall be an addendum to this policy.
- B. The administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.
- C. The school district Internet policies and procedures are available for review by all parents, guardians, staff, and members of the community.
- D. Because of the rapid changes in the development of the Internet, the school board shall conduct an annual review of this policy.

Legal References: 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. § 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)

20 U.S.C. § 1232g (Family Educational Rights and Privacy Act)
47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA))
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Mahanoy Area Sch. Dist. v. B.L., 594 U.S. ____ , 141 S. Ct. 2038 (2021)
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969)
United States v. Amer. Library Assoc., 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)

Cross References:

MSBA/MASA Model Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
MSBA/MASA Model Policy 406 (Public and Private Personnel Data)
MSBA/MASA Model Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
MSBA/MASA Model Policy 506 (Student Discipline)
MSBA/MASA Model Policy 514 (Bullying Prohibition Policy)
MSBA/MASA Model Policy 515 (Protection and Privacy of Pupil Records)
MSBA/MASA Model Policy 519 (Interviews of Students by Outside Agencies)
MSBA/MASA Model Policy 521 (Student Disability Nondiscrimination)
MSBA/MASA Model Policy 522 (Title IX Sex Nondiscrimination Grievance Procedures and Process)
MSBA/MASA Model Policy 603 (Curriculum Development)
MSBA/MASA Model Policy 604 (Instructional Curriculum)
MSBA/MASA Model Policy 606 (Textbooks and Instructional Materials)
MSBA/MASA Model Policy 806 (Crisis Management Policy)
MSBA/MASA Model Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)

**Independent School Dist. #118
Network Acceptable Use and Responsibility Policy Agreement
Regulation**

(District Policy 524 – Internet Acceptable Use and Safety is posted in the policy manual on the District website: www.isd118.k12.mn.us)

Please read the following carefully before signing this document. This is a legally binding agreement and must be signed before you will be given an access account.

Independent School Dist. #118 supports instruction through the use of educational and administrative computers, school licensed software and other media, as well as networks and servers. Independent School Dist. #118 provides Internet access. The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual people. Students, teachers, support staff, parents and school board members have limited access to: (1) electronic mail (e-mail) communication with people all over the world; (2) information and news from a variety of sources and research institutions; (3) public domain and shareware software; (4) discussion groups on a wide variety of educational topics; (5) access to many university libraries, the Library of Congress, and more!

With access to computers and people all over the world comes the availability of some material that may not be considered to be of educational value within the context of the school setting. Independent School Dist. #118 has

taken precautions to restrict access to controversial materials. However, on a global network such as the Internet, it is impossible to control the content of all available materials. Independent School Dist. #118 firmly believes that the valuable information and interaction available on this worldwide network far outweigh the possibility of users accidentally procuring material that is not consistent with the educational goals within each school.

Following are guidelines provided to establish the responsibilities of anyone using Independent School Dist. #118s' computers, media, computer networks and/or Internet access. Use of Network accounts is a privilege. If a user violates any of these provisions, his or her access may be terminated, and any future access could be denied. **The signature(s) at the end of this document is (are) legally binding and indicate(s) the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance. Any user who violates the terms of this policy will immediately lose his/her access privileges and may be subject to a hearing before the school board, and/or further legal action.**

TERMS AND CONDITIONS

I. ACCEPTABLE USE: The purpose of the Independent School Dist. #118s' networks connections are to support research and instruction, or the business of conducting education, by providing access to unique resources and opportunities for collaborative work. The use of an account must be in support of education and research, or the business of conducting education, consistent with the educational objectives of the Independent School Dist. #118 system. Additionally, use of other organizations' networks or computing resources must comply with rules appropriate for that network. Transmission of any material in violation of any U.S. or state law or state agency provisions is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material, or material protected by trade secret. Use for any non-educational purpose (as defined by Independent School Dist. #118) or commercial activity by any individual or organization, regardless of for-profit or not-for-profit status, is not acceptable. Use for product advertisement or political lobbying is strictly prohibited. (Initial) _____

II. PRIVILEGES: The use of network accounts and access to the Internet is a PRIVILEGE, not a right, therefore, inappropriate use may result in a cancellation of those privileges. Each student who receives access will be part of a discussion with an Independent School Dist. #118 faculty member pertaining to the proper use of the network. Independent School Dist. #118 administration and the system administrator(s) will deem what is inappropriate use. The decision of the system administrator(s) is final. The system administrator(s) may close an account or deny access at any time. Based on the recommendation of teachers and staff, the administration of Independent School Dist. #118 Schools may request that the system administrator deny, revoke, or suspend specific user accounts or access. (Initial) _____

III. The Educational Technology Committee firmly believes that the best security system for monitoring student acceptable use of the Internet is direct adult supervision.

. It is strictly forbidden for a staff member to give any student his/her password and/or any password.

Any student or staff member that actively compromises any security system may be held personally liable for district expenses to repair and/or replace said security system.

IV. NETIQUETTE (NETWORK ETIQUETTE) and PROTOCOLS: The use of an account or access to the Internet on any Independent School Dist. #118 network requires that you abide by accepted rules of network etiquette, which include, but are not limited to, the following:

1. BE POLITE. Do not send abusive messages to ANYONE.
2. APPROPRIATE LANGUAGE. In all messages, do not swear, use vulgarities or any other inappropriate language.
3. APPROPRIATE ACTIVITIES. Anything pertaining to illegal activities is strictly forbidden. Any activity not directly related to the educational mission of Independent School Dist. #118 is strictly forbidden. Activities relating to, or in support of, illegal activities will be reported to appropriate authorities.
4. PRIVACY. Do not reveal the personal address or phone numbers of yourself or any persons. All communications and information accessible via the network should be assumed public property. Electronic mail is

not guaranteed to be private. Systems administrators have access to all mail. Messages relating to, or in support of, illegal activities will be reported to appropriate authorities.

5. CONNECTIVITY. Do not use the network in such a way that would limit or disrupt the use of the network by others.

6. SERVICES. Independent School Dist. #118 will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors, or omissions. Use of any information obtained via networks is at user's risk. Independent School Dist. #118 specifically denies any responsibility for the accuracy or quality of information obtained through its network services.

7. SECURITY. Security on any computer system is a high priority. If users can identify a security problem on any of the networks, they must notify a system administrator either in person or via the network as soon as possible. Users must not demonstrate the problem to other users. Use of network service accounts provided by Independent School Dist. #118 is not transferable or assignable. Any user who knowingly allows another to use the account assigned to them will immediately lose their access privileges and may be subject to further legal action. Attempts to fraudulently log in on any network as a system administrator or another user will result in immediate cancellation of user privileges and may be subject to further legal action. Any user identified as a security risk or having a history of problems with other computer systems, may be denied access to the networks and other computer services.

8. VANDALISM AND ELECTRONIC MISCHIEF. Vandalism will result in cancellation of privileges. This includes, but is not limited to, electronic mischief, the uploading or creation of computer viruses, attempts to tamper with any program, applications, files, etc.

9. UPDATES. Independent School Dist. #118 may occasionally require new registration and account information from users to continue providing services. Users must notify the system administrator(s) of any changes in account information.

10. Users will not conduct personal business on district owned computers during the established workday.

Staff members will not use district owned computers for recreational use during established work hours.

11. Students must not be permitted to play non-educational games .

. Routinely allowing students to play games is strictly prohibited. However, it is permissible, to allow a class and/or student as a reinforcer to use educationally related programs or sites.

All Terms and Conditions as stated in this document are applicable to any Independent School Dist. #118 network. These Terms and Conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These Terms and Conditions shall be governed and interpreted in accordance with the laws of the State of Minnesota, United States of America.

“I understand and will abide by the above Terms and conditions for the privilege of accessing the Internet or having an account on any Independent School Dist. #118 network server. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action and/or appropriate legal action may be taken.”

Username (please print): _____

User Signature: _____ Date: _____

**** If user is under the age of 18, a parent or guardian must also read, agree to, and sign this agreement.**

PARENT OR GUARDIAN NETWORK RESPONSIBILITY AGREEMENT

As the parent or guardian of this student I have read the Terms and Conditions of Independent School Dist. #118's Network Acceptable Use and Responsibility Agreement for network services. I understand that this access is designed for educational purposes, and Independent School Dist. #118 has taken available precautions to eliminate controversial materials. However, I also recognize it is impossible for Independent School Dist. #118 to restrict access to all controversial materials, and I will not hold them responsible for materials available on the network.

Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give my permission to issue an account in my name for my child's use and certify that the information contained on this form is correct.

Parent or Guardian (please print): _____

Signature: _____ Date: _____

SPONSORING TEACHER AGREEMENT *(This is to be used only when parent/guardian is not available to authorize access to the internet)*

I have read the Terms and Conditions of Independent School Dist. #118's Network Acceptable Use and Responsibility Agreement for network services and agree to promote this agreement with the user. As the sponsoring teacher, I agree to instruct the student on acceptable use of the network and proper network etiquette.

Sponsor's Name (please print): _____

Signature: _____ Date: _____

Loss of Privileges: Upon loss of privileges under this policy, the acceptable use agreement on file at that time will be revoked.

Reinstatement: Before reinstatement can occur, a new acceptable use agreement must be signed by the parent and student.