FARMINGTON SCHOOL DISTRICT NO. 192	*ISD 192 Policy 1003* *Orig. 1995* *Revised: 11-2022* *Adopted: 01-2014*
POLICIES AND REGULATIONS	

ISD 192 SPECIFIC POLICIES

1003 ACCEPTABLE USE OF DISTRICT TECHNOLOGY

I. INTRODUCTION

The use of Independent School District No. 192 computers, computer networks, and Internet resources is a key element of the curriculum and instruction in Independent School District No. 192. The Independent School District No. 192 computer network is intended for educational purposes. Independent School District No. 192 expects that staff will incorporate appropriate use of computer network and Internet resources into the curriculum and will provide guidance and instruction to students as to their uses.

Despite its tremendous educational potential, the Internet also presents the potential for security vulnerabilities and user abuse. For safety purposes, Independent School District No. 192 employs methods to protect network resources and users. The school board expects all employees and students to abide by procedures set forth below governing the use of Independent School District No. 192's computers, computer networks, and Internet resources. Failure to follow the guidelines may result in disciplinary action. Independent School District No. 192 is not responsible for ensuring the accuracy or usability of any information found on external networks.

Parent(s)/guardian(s) will be given the opportunity to determine their child's access to the Internet when they first begin school in Independent School District No. 192. Students in Grades K-12, along with their respective parent(s)/guardian(s), will annually acknowledge their understanding of the District's Acceptable Use Policy. Independent School District No. 192 will not be responsible for any and all claims arising out of or related to the usage of this interconnected computer system.

II. ACCESS

A. Independent School District No. 192 offers Internet access for staff and student use. This policy sets for the online acceptable use procedures for all staff and students using the district's computers and network. This acceptable use policy applies to all technologies capable of accessing, inputting, or extracting information/data from the district's computer network, electronic mail (e-mail), and Internet.

B. Students and employees shall have access to Internet information resources through computers and mobile devices located in their classroom, library, computer lab, office, or other location.

C. Students and their parent(s)/guardian(s) must sign an Acceptable Use Consent form to be granted access to the Internet via the Independent School District No. 192 computer network.

D. Signatures are required annually acknowledging agreement with the Acceptable Use of District Technology, Policy 1003. Student signatures, as appropriate, along with parent/guardian signatures will be required annually for learners in Grades K-12. Parent(s)/guardian(s) can withdraw their approval at any time.

E. The school district shall provide each employee, where appropriate, an email account, learning management system account, telephone and voicemail account, and file/cloud storage allocation along with collaborative online workspace accounts.

F. The school district shall provide each student, where appropriate, an email account, learning management system account, networked data storage allocation, district cloud-based storage and collaborative apps.

G. The use of the school district technology systems and access to the Internet is a privilege, not a right. The school district reserves the right to limit or remove any user's access to the school district's computer system, equipment, email/voicemail system, and Internet access at any time. Depending on the nature and degree of a violation and the number of previous violations, unacceptable use of a 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; loss of credit and/or reduction of grade; discipline under other appropriate school district policies including suspension, expulsion, exclusion, or termination of employment; or civil or criminal liability under other applicable laws.

III. EDUCATIONAL PURPOSE

A. The Independent School District No. 192 computer network has not been established as a public access service and is not an "open" or "limited open" forum. The term "educational purposes" includes, but is not limited to, information management, classroom activities, media-center projects, educational research, career development, and curriculum activities using computers and Internet resources.

B. The Independent School District No. 192 computer network has not been established as a public access service or a public forum. Independent School District No. 192 has the right to place reasonable restrictions on the material accessed or posted through the system into the intranet, email, voicemail, web sites, list server, blog site, or other school district system. Students and employees are expected to follow the rules set forth in this policy and the law when using the Independent School District No. 192 computer network and Internet resources. Network activity may be monitored to ensure educational utilization and compliance with policy and law.

C. Students and employees may not use the Independent School District No. 192 computer network for non-educational or commercial purposes. This means that no products or services may be offered, provided, or purchased through the district computer network, unless such products or services are for a defined educational purposed and such activity has been approved by the Superintendent or designee.

D. Independent School District No. 192 computers may not be used for political lobbying but may be used to communicate with elected representatives and to express opinions to them on political issues.

E. Employees and School Board members shall utilize the school district-assigned email account for all email communication related to their roles with Independent School District No. 192. Employees and School Board members should avoid use of the school district-assigned email account for electronic solicitation, distribution of "chain letters," sending the messages unrelated to job role to large numbers of recipients, or for any commercial purpose.

F. Independent School District No. 192 may offer network and Internet resources to guests and visitors to school facilities. This guest access, whether made available through wired or wireless network, does not establish an open, limited open, or public forum. All guidelines of this policy apply to students and employees accessing network or Internet resources through the school district guest access, sometimes referred to as "Wi-Fi." Users other than students and employees must agree to "Terms of Use" prior to use of guest access.

IV. YOUR RIGHTS AND RESPONSIBILITIES

A. Free Speech

A student's right to free speech applies to communication on the Internet. Independent School District No. 192 computer network is considered a limited forum, similar to the school newspaper, and, therefore, the district may restrict speech for valid educational reasons. The district shall not restrict speech on the basis of a disagreement with the opinions expressed.

B. Search and Seizure

1. Students and employees should not expect any privacy in the contents of personal files on the district systems. Administrators and faculty may review files and messages to maintain system integrity and ensure that users are acting responsibly.

2. The district may examine all information stored on district technology resources at any time. The district may monitor staff and student technology usage. Electronic communications, all data stored on the district's technology resources, and downloaded material, including deleted files, may be intercepted, accessed, or searched by a district administrator or designees at any time.

3. Routine maintenance and monitoring of Independent School District No. 192 technology systems may lead to discovery that this policy or other school board policies and/or federal, state, or local laws have been violated.

4. An individual search shall be conducted if there is reasonable suspicion that this policy, school board policies, and/or laws have been violated. The investigation shall be reasonable and related to the suspected violation.

5. Parent(s)/guardian(s) of students have the right at any time to request to see the contents of student's files stored on school district technology systems.

C. District Employees

Rights, responsibilities, and duties of district employees as they relate to school district network and Internet resources are governed by the school board policies and procedures, applicable individual agreements between the employee and the school district, and applicable master agreements between the district and the employee bargaining units. Employees may be disciplined or terminated for violating the district's policies, regulations, and procedures.

D. Due Process

The district shall cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through Independent School District No. 192 computer network.

V. UNACCEPTABLE USES

The following uses of the Independent School District No. 192 computer network and Internet resources are considered unacceptable:

A. Personal Safety

1. Students and employees shall not post or provide personal contact information about themselves or other people on the Internet without the consent of the subject of the information. Personal contact information includes a student's or employee's home address or telephone number.

2. Student shall not agree to meet with someone contacted or met using school district network resources without parent's approval.

3. Students shall promptly disclose to their teacher or other school employee any content viewed using school district network resources that is inappropriate or causes discomfort.

B. Illegal Activities

1. Students and employees shall not attempt to gain unauthorized access to Independent School District No. 192 computer network or to any other computer system through Independent School District No. 192 computer network or go beyond authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing."

2. Students and employees shall not make deliberate attempts to disrupt the computer systems or destroy data by spreading computer viruses, adware, malware, or by any other means. These actions are illegal, and criminal prosecution and /or disciplinary action will be pursued.

3. Students and employees shall not use Independent School District No. 192 computer network system to engage in any act that is illegal; that facilitates gambling; or that violates any local, state, or federal statute. Students and staff shall not use the Internet or the school district's computer network to harass, bully, or threaten the safety of others.

4. Misuse of the school district's computer equipment or network including but not limited to, deletion or violation of password protected information, computer programs, data, password or system files; inappropriate access of files, directories, Internet sites; deliberate contamination of system unethical use of information, or violation of copyright laws is prohibited.

5. Physical abuse or tampering with school district computer, telecommunications, or network equipment is prohibited. Such abuse or tampering will be considered vandalism, destruction, and defacement of school district property.

C. System Security

1. Employees are responsible for their individual email, voicemail, file directory, and shared directory accounts and should take all reasonable precautions to prevent others from being able to use their accounts. If the need arises to share access to such accounts, contact the technology department. Unless authorized, staff should not provide their login identity and/or passwords to another person.

2. Students shall immediately notify a teacher or administrator if they have identified a possible security problem in the school district network or Internet resources. Students should not look for security problems, because this may be construed as an illegal attempt to gain access. Under no conditions should students provide other students with their login identity and/or network password.

3. Students and employees shall avoid the inadvertent spread of computer viruses by following all school district procedures related to introducing downloaded files or software, file storage devices, or other hardware or software brought into the school from outside.

4. Students who gain access to teacher computer files, directory, programs, and web site without permission from a teacher may be disciplined.

5. Tampering with the school district's computer security system, and /or applications, and/or documents, and/or equipment will be considered vandalism, destruction, and defacement of school property. Please be advised that it is a federal offense (felony) to break into any security system. Financial and legal consequences of such actions are the responsibility of the user and/or student's parent or guardian.

D. Inappropriate Language

1. Restrictions against inappropriate language apply to public messages, private messages, material posted on web pages, social networking sites, and other school district network or Internet resource capable of electronic communication.

2. Students and employees shall not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or graphic representations of such language.

3. Students and employees shall not post information that could cause damage or a danger or disruption.

4. Students and employees shall not engage in personal attacks, including prejudicial or discriminatory attacks, based on a person's race, gender, sexual orientation, religion, national origin, or disability, or engage in any other harassment or discrimination prohibited by school district policy or by law.

5. Students and employees shall not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If students or staff are told by a person to stop sending them message or otherwise communicating with them, they must stop.

6. Students and employees shall not knowingly or recklessly post false or defamatory information about a person or organization.

E. Respect for Privacy

1. Students and employees shall not repost or forward a message that was sent to them privately without permission of the person who sent them the message.

2. Students and employees shall not post private information about another person on the Internet. This does not prohibit staff from discussing private student information with each other or with a student's parent or guardian via email or voicemail, in conformance with laws and policy governing data practices.

F. Respecting Resource Limits

1. Students and employees shall use the system only for educational and career development activities and Independent School District No. 192 curriculum activities.

2. Students and employees will have access to limited space on the school district's storage media. Student ability to download files shall be limited by applicable school district procedures. Student files may be deleted without notice if such files do not support the instructional process or are exceedingly large. Users are responsible for making backup copies of files that are critical to their use.

3. Student and employees shall not post or forward chain letters. Students and employees shall not engage in spamming. (Spamming is sending an annoying or unnecessary message or solicitation to a large number of people.)

4. Students shall not deliberately or knowingly delete another student's or employee's file.

5. Students and employees shall only use software, including but not limited to email applications and web browsers, that is supplied by the school district. Employees and students shall not install hardware or software or reconfigure equipment on the school district's technology systems without express permission from the Technology Coordinator

6. Staff and students must not be wasteful of district resources including but not limited to toner and paper.

G. Plagiarism and Copyright Infringement

1. Students and employees shall not plagiarize works that are found on the school district's network or Internet resources. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.

2. Students and employees shall respect the rights of copyright owners. Copyright infringement occurs when one inappropriately reproduces a work that is protected by copyright. If a work contains language that specifies appropriate use of that work, follow the expressed requirements. If unsure whether or not work can be used, request permission from the copyright owner. Copyright law covers a myriad of resources including

music and film. Copyright law can be very confusing; ask media specialist for guidance as needed.

H. Inappropriate Access to Material

1. Students and employees shall not use the Independent School District No. 192 computer network, District-provided device, or student-owned device used at school to access or create material that is profane or obscene (pornography), contains viruses, network hacking programs, or similar programs that advocate illegal acts, or that advocate violence or discrimination towards other people (hate literature).

2. If students mistakenly access inappropriate information, they should immediately tell their teacher, media specialist, or another district employee. This will protect them against claims that they have intentionally violated this policy.

3. Parent(s)/guardian(s) should instruct students if there is additional material they think is inappropriate for students to access. The district fully expects that students shall follow their parent's instructions in this matter while using District-provided technology at home.

4. Educators will monitor student use of the Internet in schools and will take reasonable measures to prevent access by students to inappropriate materials on the Internet and restrict access to materials harmful to students.

5. Parents will monitor student use of the Internet at home and will take reasonable measures to prevent access, by students, to inappropriate material on the Internet and restrict access to material harmful to students.

6. The district may monitor the online activities of employees and students and operate technology protection measures (blocking devices or software) on the network as required by law. These measures will attempt to protect against access to visual depictions that are obscene, harmful to students, and child pornography, as required by law. Evasion or disabling of the blocking/filtering device or software installed by the school district, including attempts to evade or disable, is a violation of the acceptable use policy.

VI. LIMITATION OF LIABILITY

Independent School District No. 192 makes no warranties of any kind, either expressed or implied, related to school district network or Internet resources. The school district does not assume and, hereby, expressly disclaims liability for the misuse of its computers, equipment, email, voicemail, network or Internet resources that violate this policy or any applicable law. The district makes no guarantee that the functions or the services provided by or through the district system shall be error-free or without defect. The district is not responsible for any damage suffered through the use of its computer system, including but not limited to, the loss of data, interruptions of service, the

accuracy or quality of information obtained through or stored in the system, damage to property used to access school district computers or online resource, or financial obligations resulting from the use of school district resources.

VII. 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.

VIII. 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 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 or guardian 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.

IX. 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 to whom the school has an individualized family service plan, an individualized education program, or a 504 plan in effect.

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)
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 89 S.Ct. 733, 21 L.Ed.2d 731 (1969)
United States v. Amer. Library Assoc., 539 U.S. 194, 123 S.Ct. 2297, 56 L.Ed.2d 221 (2003)
Doninger v. Niehoff, 527 F.3d 41 (2nd Cir. 2008)