Adopted: 4/22/13, 5/23/95

Revised: 4/22/13, 3/27/06, 1/26/98, 4/23/96

517 POLICY ON DISTRICT-PROVIDED ACCESS TO ELECTRONIC INFORMATION, SERVICES, AND NETWORKS

I. PURPOSE

The purpose of this policy is to set forth guidelines for access to acceptable and safe use of the Cloquet Public Schools electronic technologies. Electronic technologies include but are not limited to computers and peripherals, printers, telephones, and the applications they support and/or access. The purpose of district-provided Internet access is to facilitate communications in support of research and education.

II. GENERAL STATEMENT OF POLICY

The Cloquet School District provides technology resources to its students, staff, parents and community for educational, administrative, and informational purposes. The goal of providing these resources is to promote educational excellence in Cloquet schools by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers and support staff.

III. LIMITED EDUCATIONAL PURPOSE

Access to the technology in the Cloquet School district has been established for educational purposes. The school district is providing students and employees with access to the school district's 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 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 the limited-purpose network. All electronic technologies must be used in support of the educational program of the District.

IV. DEFINITIONS

The term "users" refers to any person using the District's electronic technologies.

The term "Internet" refers to an electronic communications network that connects computer networks and organizational computer facilities around the world.

The term "intranet" refers to all District network(s) which restricts access to authorized users, which may include students, staff, parents, contractors, vendors and volunteers.

V. RESPONSIBILITY OF USE

School computers, telecommunications, memory devices, networks, and related hardware and software are the property of the Cloquet School District. At no time does the District relinquish its exclusive control of electronic technologies. Inappropriate use of District electronic technologies, including interfering with the network functions and the standardization of technologies, may result in the limitation or revocation of access.
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 my result in one or more of the following consequences: suspension or cancellation of use or access privileges; payment 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.

A. Users are prohibited from using school district Internet resource/accounts for the following purposes:

1. 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; or

   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. To knowingly or recklessly post, transmit, or distribute false or defamatory information about a person or organization, to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

3. To engage in any illegal act or violate any local, state, or federal statute.

4. To vandalize, damage, or disable the property of another person or organization; to make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means tamper with, modify or change the school district system software, hardware, or wiring; or to take any action to violate the school security system or use the school district system in such a way as to disrupt the use of the system by other users. Users may not add or remove any software nor modify the equipment, software, configuration, or environment. All electronic technology requests must go through the District's Technology Department processes.

5. To gain unauthorized access to information resources or to another person's materials, information, or files without the implied or direct permission of that person.

6. 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.

7. 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. To violate copyright laws or usage licensing agreements, or otherwise use another person's intellectual 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. 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 gods 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.

B. 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 should 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.

C. The Cloquet School District does not support personal equipment. Users will not install any personal equipment or software on any district-owned systems.

D. Ethical use Expectations

1. Use of school district Internet access is limited to educational purposes such as research, professional development, instruction, and collaborative projects.

2. Users will protect individual accounts by keeping passwords secure, not using another person's account, and reporting any security problems to a teacher, principal, supervisor, or other appropriate authority.

3. The school district is not responsible for unauthorized financial obligations resulting from staff or student users of the Internet access accounts.

4. Users storing information on district diskettes, hard drives, or servers do so at their own risk.

5. All users will use school district services and facilities in a manner that does not interfere with or disrupt other network users, services, or equipment. Such prohibited interference or disruption includes, but is not limited to:

   a. Wide-scale distribution of messages to forums or mailing lists unrelated to current classroom topics.

   b. Propagation of computer viruses or worms.

   c. Use of the network to make unauthorized entry into other computational information or communication devices or resources. (This includes unauthorized security probing activities or other attempts to evaluation security integrity of a network or host system.)

6. Vandalism or harassment will not be tolerated.

Vandalism is defined as any intentional attempt to harm, modify, or destroy data of another user, Internet, school district, or other networks that are connected to the school district network. This includes, but is not limited to, the uploading or creating of computer viruses.

Harassment is defined as the persistent annoyance of another user, or the interference in any way of another user's work. Harassment includes but is not limited to the sending of unsolicited mail.

7. Obstructing other users' work by consuming excessively large amounts of system resources (disk space, CPU time, bandwidth), wasting technology resources (toner, ink cartridges, supplies) or by deliberately crashing the machine (s) will not be tolerated and is subject to discipline.

VI. FILTERS

A. With respect to any of its computers with Internet access, the School District will monitor online activities of minors 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 obscene, violent, child pornography, or 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 the prurient interest in nudity, violence, 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. An administrator, supervisor, or other person authorized by the Superintendent may disable the technology protection measure, during the use by an adult, to enable access for bona fide research or other lawful purposes.

D. The District is obligated to monitor and/or review filtering activities.

E. The District implements several methods to help protect the network from harmful viruses and reduce the amount of SPAM email (email filter, firewalls, etc.). A privacy disclaimer is attached to all outgoing email messages. All these methods address the need to keep our system operational and protect the district from lawsuits.

VII. LIMITED EXPECTATION OF PRIVACY

By authorizing use of the School District electronic technologies, the Cloquet School District does not relinquish control over content or data transmitted or stored on the network or contained in files. Users should expect only limited privacy in the contents of personal files on the District's electronic technologies.

A. Routine maintenance and monitoring of the district's electronic technologies may lead to a discovery

that a user has violated this policy, another School District policy, or the law.

B. 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.

C. The telecommunications network and equipment is owned and operated by the school district for the expressed use of staff and students in education-related activities. The district retains the right to monitor activity of users consistent with the law.

D. Parents have the right at any time to investigate or review the contents of their child's files. Parents have the right to request the termination of their child's individual account at any time.

E. District staff is advised 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, District staff is advised that data and other materials in files maintained on or transmitted through the District's electronic technologies may be subject to review, disclosure or discovery under the Minnesota Government Data Practices Act.

F. The 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 districts electronic technologies.

G. Web Publishing - when publishing content to third-party sites, including web pages and web logs (BLOGs), all policies and guidelines of the District apply. Teachers assume responsibility of having students adhere to these guidelines.

H. Student E-mail accounts

1. The school district does not provide for or allow student e-mail accounts.

2. In cases like special projects, when students may use e-mail accounts generated through outside sources (AOL, Yahoo), the Acceptable Use Policy applies to e-mail generated by the student.

VIII. ELECTRONIC TECHNOLOGIES ACCEPTABLE 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 staff of the 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. The Electronic Technologies Acceptable Use Agreement for students must be read and signed by the user and parents or guardians. The employee must sign the Internet Use Agreement for employees. The form must then be filed with the district.

D. All users shall be responsible for the protection and security of their passwords. Users shall have the ability to change passwords to maintain the confidentiality of logon codes.

IX. LIMITATION ON SCHOOL DISTRICT LIABILITY

Staff, Students and District Guests may use personal devices to access the Cloquet School District Guest WiFi network/SSID. Access to the "GUEST CLOQUET SCHOOLS" WiFi network/SSID does not guarantee the privacy of your data and communication while using this Service. There are potentially serious issues with any computer connected to the Internet without the appropriate security protection, ranging from viruses, worms and other programs that can damage the users computer, to attacks on the computer by unauthorized or unwanted third parties. By using this Service, you acknowledge and knowingly accept these

potentially serious risks of accessing the Internet over an unsecured network. It is recommended that users take steps to protect their own computer system, such as installing current anti-virus software and maintaining appropriate firewall protection on their computer devices.

Use of the District's educational technologies is at the user's own risk and is provided on an "as is, as available" basis. The District will not be responsible for any damage users may suffer, including but not limited to, loss, damage or unavailability of data stored on the District's systems or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The District is not responsible for the accuracy or quality of any advice or information obtained through or stored on the District's electronic technologies. The District will not be responsible for financial obligations arising through unauthorized use of the District's educational technologies or the Internet. The District does not promise that any particular level or method of access will be given or continued and retains the authority to qualify, limit, or terminate any or all telecommunication, Internet, or computer use. District networks are private networks used as an education tool by employees and students. District computer networks are monitored electronically.

X. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the District's electronic technologies shall be consistent with school district policies and the mission of the Cloquet Public Schools.

XI. USER NOTIFICATION

All users shall be notified of the guidelines and policies governing district computer network use.
This notification shall include:

A. Disclaimers limiting the school district's liability relative to:

1. Information stored on school district diskettes, hard drives, or servers.

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

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

4. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet. Such obligations incurred by a student through the Internet are the sole responsibility of the student and/or the student's parents.

B. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.

C. Notification of password ownership and password protection procedures.

D. Notification that, should the user violate the Acceptable Use Policy, the users access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

E. Notification that, even though the district may use technical means to limit student Internet access, these limits are not impenetrable and are not the sole means of enforcing the provisions of the Acceptable Use Policy.

F. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by School Board Policy 406, Public and Private personnel Data, and School Board Policy 515, Protection and privacy of Pupil Records.

G. Notification that all provisions of the 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 televisions, telephones, radio, movies and other possibly offensive media. Parents/guardians 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 or information resources from home or a remote location.

B. Parents/guardians will be notified that their students will be using District resources/accounts to access the Internet and that the District will provide parents the option to request alternative activities not requiring Internet access. This notification should include:

1. A copy of the Acceptable Use Agreement 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 Acceptable Use Agreement must be signed by the user, parent or guardian, and the supervising teacher prior to use by the student; and

5. A statement that the District's Acceptable Use Policy is available for parental review.

C. This regulation requires that all electronic resources and materials be consistent with adopted guidelines; supporting and enriching the curriculum while taking into account the varied instructional needs, learning styles, and abilities of the students. Access to telecommunications will enable students to explore thousands of libraries, databases and resources.

D. On a global network, it is impossible to effectively control the content of data. The District will employ appropriate mans available to attempt to limit access to inappropriate or offensive material. The School Board believes that the benefits to students from access to Internet information resources and opportunities for collaboration exceed the disadvantages. Parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources.

XII. STAFF RESPONSIBILITIES

Staff responsibilities include, but are not limited to the following:

- Develop and help students develop the skills needed to discriminate among information sources, to identify information appropriate to age and developmental levels, and to evaluate and use information to meet educational goals.
- Supervise and/or monitor all whom one grants access to technology resources regarding implementation of this policy.
- Take an active role in ensuring that students and their parents are aware of their responsibility to use technology resources in an ethical and educational manner.

XIII. STUDENT RESPONSIBILITIES

Student responsibilities include, but are not limited to the following:

- Demonstrate basic skills in computer use.
- Demonstrate an understanding of this policy.
- Have parental permission before being allowed to use the Internet or computer network.
- Be aware of the dangers of online communications with strangers.
- Report any abusive or suggestive messages or information immediately to a supervisor or monitor.

XIV. IMPLEMENTATION AND POLICY REVIEW

A. Administration may develop the necessary guidelines for the implementation of this policy. The District Administration may develop appropriate user notification forms, guidelines and procedure 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 District's Internet policies and procedures are available for review by all parents, guardians, staff and members of the community.

Legal References:

17 U.S.C. § 101 *et. seq.* (Copyrights)
15 U.S.C. § 6501 *et. seq.*
Children's Internet Protection Act of 2000 (CIPA) 47 U.S.C. § 254
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Title III of the Elementary and Secondary Education act of 1965,
20 U.S.C. § 1601, *et. seq.,* as amended
Minn. Stat. §§ 125B.15 and 125B.25
Minn. Stat. §§ 609.87, 609.88, 609.89 and 609.891
http://www.revisor.leg.state.mn.us/stats/609/

Cross References:

Policy 506 Student Discipline
Policy 406 Public and Private Personnel Data
Policy 515 Public Notice
Policy 413 Harassment and Violence
Policy 603 Curriculum and Staff Development