Internet Safety Policies and CIPA: An E-Rate Primer for Schools and Libraries

Prepared by E-Rate Central

The Children's Internet Protection Act ("CIPA"), enacted December 21, 2000, requires recipients of federal technology funds to comply with certain Internet filtering and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connection services must also meet the Internet safety policies of the Neighborhood Children's Internet Protection Act ("NCIPA") that addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities.

Introduction to CIPA Compliance

CIPA (and the associated NCIPA) requirements for E-rate purposes are governed by rules promulgated by the Federal Communications Commission ("FCC") and administrated by the Schools and Libraries Division ("SLD"). The basic FCC rules are summarized below.

1. Applicability: CIPA compliance is required for any school or library receiving E-rate funds for two of the three eligible service categories – Internet Access and Internal Connections. Applicants for Telecommunications services only, are exempt.

2. Timing: Full compliance is required in an applicant's second year of funding after CIA's enactment. For most applicants, this will be the fifth E-rate program year ("PY5") beginning July 1, 2002. For the preceding year (PY4 for most), an applicant need only certify that it is "undertaking actions" to be in compliance for the second year.

3. Filtering: CIPA requires the implementation of a "technology protection measure" – generally referred to as an Internet filter – to block access to visual depictions deemed "obscene," "child pornography," or "harmful to minors."[1] Filtering is required for all of an E-rate recipient's Internet-enabled computers whether used by minors or adults. For E-rate funding purposes, filtering for adult Internet usage can be disabled for "bona fide research or other lawful purpose."[2]

---

[1] The terms "obscene," "child pornography," and "harmful to minors" are strictly and legally defined (see footnote to the sample Internet Safety Policy in Appendix B).

[2] Although the ESEA and LSTA sections of CIPA permit the disabling of filters for both adults and minors, no such provision for minors is included in the E-rate section (SEC. 1721). No provision, however,

The FCC has not established any standards with regard to the type or effectiveness of Internet filters required for CIPA compliance.

4. Internet Safety Policy: CIPA requires the adoption and enforcement of an "Internet safety policy" covering the filtering discussed above.[3] For schools, the policy must also address "monitoring the online activities of minors."[4]

   NCIPA provisions, applicable to E-rate recipients, also require a policy to address:

   - "the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications" (including instant messaging);
   - "unauthorized access, including so-called 'hacking,' and other unlawful activities by minors online;"
   - "unauthorized disclosure, use, and dissemination of personal identification information regarding minors;" and
   - "measures designed to restrict minors' access to materials harmful to minors."[5]

   Prior to adoption, CIPA requires that "reasonable public notice" and "at least one public hearing or meeting" be held to address the proposed Internet safety policy.

   The FCC has not established any specific criteria for evaluating an Internet safety policy, nor has it set any specific standards for what constitutes reasonable public notice or a public meeting.

5. Certification: The only specific compliance requirement established by the FCC is that an E-rate applicant must certify that it is in compliance with the CIPA provisions summarized above. Certification is required only after funding is awarded by filing a Form 486 indicating receipt of services.[6] Certification is required annually.

6. Enforcement: No specific enforcement provisions, other than applicant certifications, have been established by the FCC. The only two principles of enforcement are:

---

prevents schools and libraries from setting different levels of filtering for minors on an age-determinant or individual use basis.

[3] In addition to the three types of material that must be blocked, CIPA explicitly permits schools and libraries to block any content deemed inappropriate for minors by local standards.

[4] "Monitoring" appears to require only supervision, not technical measures. Specifically, CIPA does not require "tracking of Internet usage by any identifiable minor or adult user."

[5] Not just visual depictions.

[6] Members of a consortium must certify status on Form 479s that must be submitted to the consortium leaders before the leader files a consortium-wide Form 486.

- No Universal Service Fund payments will be made on behalf of any applicant that does not file the requisite certifications; and
- If certifications are found to be false – as determined by subsequent review or audit – applicants will have to reimburse the Fund for any funds and discounts received for the period covered.

Internet Safety Policy Guidelines

Although neither the FCC nor the SLD has established specific criteria for an Internet safety policy, certain practical guidelines can be suggested as a means of complying with the CIPA policy requirements.

Basic Components of a CIPA-compliant Internet Safety Policy:

At a minimum, to fully comply with the spirit of the Internet safety policy requirements for E-rate funding, four key guidelines should be met.

1. The policy should apply to both minors and adults. Although called the "Children's Internet Protection Act," and requiring specific protections for minors, CIPA clearly applies to certain aspects of adult usage as well. Therefore, the policy should deal with both staff and students (or library patrons). As discussed below, a student Acceptable Use Policy may not fully suffice.

2. The policy should specify use of an Internet filtering mechanism to, at a minimum, block access to the three categories of visual depictions specified by CIPA – obscene, child pornography, and harmful to minors. Conditions and procedures should be incorporated under which filtering can be disabled (for adults) or made less restrictive (for minors).

3. The policy should emphasize staff responsibilities in supervising online activities by minors. This provision is needed to meet the "monitoring" requirement imposed on schools (but also appropriate for libraries).

4. The policy should address the NCIPA issues for minors (but is also appropriate for adults). As discussed above, these issues concern the safe use of e-mail and other forms of electronic messaging, unauthorized disclosure of personal information, and unlawful online activities.

A sample Internet safety policy, minimally addressing these four CIPA-related guidelines, is provided in Appendix B.

Optional Internet and Network Policy components:

The sample Internet safety policy provided in Appendix B is designed solely to meet the basic E-rate requirements for CIPA compliance. Although not the primary purpose of this Primer, it should be noted that many schools and libraries may already have, or may wish to adopt, much broader policies addressing other Internet or network issues. A brief summary of other typical policy components is provided below. Several examples of broader policies are provided in the Internet links listed in Appendix A.

1. Statement of objective. Discussion as to the purpose and importance of the organization's computer network and Internet access. Access to these resources may be designated a privilege, not a right.

2. Penalties for improper use. Failure to adhere to network policies and rules may subject users to warnings, usage restrictions, disciplinary actions, or legal proceedings.

3. Organizational responsibility and privacy. Disclaimers indicating that:
   - The organization does not warrant network functionality or accuracy of information.
   - The organization does not warrant the effectiveness of Internet filtering.
   - The privacy of system users is limited.

4. Acceptable use. Provisions dealing with such issues as:
   - Network etiquette.
   - Vandalism and harassment.
   - Copyrights and plagiarism.
   - Downloading (e.g., music files)

5. Web site. Special provisions dealing with the use and modifications of an organization's own Web site.

6. Personnel responsibilities. Designation of an organization's personnel who are responsible for various aspects of network and user administration and use.

Review and Revision of Existing Policies:

Many schools and libraries may have existing policies in place that fully, or at least partially, meet the CIPA requirements for an Internet safety policy. If a review indicates the need for a revision, the following suggestions are offered for consideration:

1. Title. To indicate CIPA compliance, it would be useful to include the words "Internet safety policy" in the title or introductory text.

2. Specific terms. Terminology may be important to CIPA compliance.

a. Prohibited activity should specifically include access to material deemed "obscene," "child pornography," or "harmful to minors."

b. Reference should be made to supervision or "monitoring" of online activities by minors.

c. References to disabling of filtering should refer to "disabling or relaxing" for "bona fide research or other lawful purposes."

3. Specific problems. Although not a CIPA issue, it may be appropriate to expand portions of earlier policies to deal more explicitly with problems recently faced by schools and libraries such as student and staff harassment, plagiarism, and copyright violations.

4. Adult usage. The policy should address usage by adults, not simply students and/or minors. Adult-oriented policies are becoming commonplace in corporate and governmental organizations to establish standards of behavior for network usage.

5. Companion policies. Schools, with an existing student-oriented acceptable use policy, may be able to adopt a broader, but simpler, Internet safety policy referencing the acceptable use policy.

6. Public hearing. Revised, CIPA-compliant, Internet safety policies should be adopted in a pre-announced public meeting. A regular school or library board meeting, at which the policy adoption is listed in a pre-released agenda, should be sufficient.

Appendices:

Appendix A – Internet links for further information

Appendix B – Sample, CIPA-compliant, Internet safety policy

3187 - Use Policy for Internet Access

A. Purpose

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

B. General Statement of Policy

In making decisions regarding student and employee access to the Duluth Public Schools' 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.

C. Limited Forum for District's Educational Use

The Duluth Public Schools 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.

D. Use of System is a Privilege

The use of the Duluth Public Schools' 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.

Guidelines for Internet Access use are contained in Regulation 3187R.

Internet Safety

A. Introduction

It is the policy of the Duluth Public Schools to:

(1) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;

(2) prevent unauthorized access and other unlawful online activity;

(3) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

(4) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

B. Definitions

Key terms are as defined in the Children's Internet Protection Act.

C. Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

D. Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the Duluth Public Schools online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:

(1) unauthorized access, including so-called 'hacking,' and other unlawful activities; and

(2) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

E. Supervision and Monitoring

It shall be the responsibility of all members of the Duluth Public Schools staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Department or designated representatives.

F. CIPA definitions of terms:

TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

(1) OBSCENE, as that term is defined in section 1460 of title 18, United States Code;

(2) CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code; or

(3) Harmful to minors.

HARMFUL TO MINORS. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

(a). Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

(b). 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

(c). Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

(4) SEXUAL ACT; SEXUAL CONTACT. The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

REFERENCES:
E-rate Central sample CIPA Internet Safety Policy
Children's Internet Protection Act

Legal References:
15 U.S.C. § 6501 *et seq.* (Children's Online Privacy Protection Act)
17 U.S.C. § 101 *et seq.* (Copyrights)
20 U.S.C. § 6751 *et seq.* (Enhancing Education through Technology Act of 2001)
47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA))
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Minn. Stat. § 125B.15 (Internet Access for Students)
Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 89 S.Ct. 733,21 L.Ed.2d 731 (1969)
United States v. American Library Association, 539 U.S. 194, 123 S.Ct.2297, 56 L.Ed.2d 221 (2003)
Layshock v. Hermitage Sch. Dist., 412 F.Supp. 2d 502 (2006)
J.S. v. Bethlehem Area Sch. Dist., 807 A.2d 847 (Pa. 2002)

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 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 (Student Sex Nondiscrimination)
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)

Adopted:	12-16-97	ISD709
Revised:	7-17-2001	
Revised:	6-12-2007	
Adopted:		
Revised:	5-13-2008	

3187R – INTERNET USE REGULATIONS

A. Appropriate Use of Technology Resources for Students

These regulations pertain to the use of District and personal technology resources while on school property, in school vehicles and at school-sponsored activities, as well as the use of District technology resources via off-campus remote access.

(1) Introduction

The Duluth Public Schools is pleased to offer students access to District computers, communications systems[1], the Internet and an array of technology resources to promote educational excellence. Each student is responsible for his/her use of technology, whether personal or District-provided. While using District and personal technology resources on school property, in school vehicles and at school-sponsored activities, as well as using District technology resources via off-campus remote access, each student must act in an appropriate manner consistent with school, District, and legal guidelines in this limited forum. It is the joint responsibility of school personnel and the parent or guardian of each student to educate the student about his/her responsibilities and to establish expectations when using technology.

(2) Using the Internet and Communications Systems[1]

District technology resources are provided to students to conduct research, complete assignments, and communicate with others in furtherance of their education.

(a) Access is a privilege not a right; as such, general rules of school behavior apply.
(b) Access to these services is given to students who agree to act in a considerate and responsible manner. Just as students are responsible for good behavior in a classroom or a school hallway, they must also be responsible when using school computer networks or personal technologies.
(c) Students must comply with District standards and honor this agreement to be permitted the use of technology.
(d) All digital storage is District property, and as such, network administrators will review files and communications to maintain system integrity and ensure that students are using technology responsibly.
(e) Students should not expect that files stored on District servers will be private.
(f) The educational value of technology integration in curriculum is substantial. Access to the Internet will enable students to use extensive online libraries and databases.
(g) Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, profane, sexually oriented or potentially offensive to some people. While the intent is to make Internet access available to further educational goals and objectives, students may find ways to access these other materials as well. The Duluth Public Schools does not condone or permit the use of this material and uses content filtering software to protect students to the extent possible.
(h) Parents and guardians must be aware that content filtering tools are not completely fail-safe and while at school, direct supervision by school personnel of each student using a computer is desired but not always possible.
(i) Students are expected to use technology resources in a manner consistent with the rules below and will be held responsible for their intentional misuse.

(j) The Duluth Public Schools believes that the benefits of student access to the Internet in the form of information resources and opportunities for collaboration exceed any disadvantages.
(k) Ultimately, parents and/or guardians are responsible for setting and conveying the standards that their children should follow when using technology. If a student accidentally accesses inappropriate material they should back out of that information at once and notify the supervising adult.

(3) Proper and Acceptable Use of All Technology Resources

All District technology resources, including but not limited to District computers, communications systems[1] and the Internet, must be used in support of education and academic research and must be used in a manner consistent with the educational mission and objectives of the Duluth Public Schools.

Activities that are permitted and encouraged include:

(a) school work;
(b) original creation and presentation of academic work;
(c) research on topics being studied in school;
(d) research for opportunities outside of school related to community service, employment or further education

Activities that are not permitted when using District or personal technologies include but are not limited to:

(a) plagiarism or representing the work of others as one's own;
(b) any activity that violates a school rule or a local, state, federal, or copyright law;
(c) using obscene language; harassing, insulting, ostracizing, cyber bullying or intimidating others;
(d) representing Copyright ©, Registered ®, and/or Trademark ™ materials as one's own work;
(e) searching, viewing, communicating, publishing, downloading, storing, or retrieving materials that are not related to school work, community service, employment, or further education (thus, searching inappropriate materials is not permitted);
(f) damaging or modifying computers, networks or District-installed software;
(g) intentional or neglectful transmission of viruses or other destructive computer files; hacking into District or external technology systems; intentionally bypassing District filters;
(h) use of USB, bootable CDs, or other devices to alter the function of a computer or a network;
(i) subscription to any online services or ordering of any goods or services;
(j) use of personal e-mail accounts, not District-provided e-mail accounts, on the District network;
(k) online sharing of any student's or staff member's name, home address, phone number or other personal information;
(l) non-educational uses such as games, role-playing multi-user environments, gambling, junk mail, chain mail, jokes or raffles;
(m) participating in online chat rooms or using instant messaging, unless specifically assigned by a teacher;

(n) use of District resources for commercial purposes, personal financial gain, or fraud, including but not limited to any activity that requires an exchange of money and/or credit card numbers, any activity that requires entry into an area of service for which the school will be charged a fee, any purchase or sale of any kind; and any use for product advertisement or political lobbying;
(o) any activity that requires entry into an area of service for which the school will be charged a fee, any purchase or sale of any kind; and any use for product advertisement or political lobbying;
(p) accessing or attempting to access instant messages, chat rooms, forums, e-mail, message boards, or hosting personal web pages during the instructional day. Teachers may authorize students to use Internet communication that includes filtered email for instructional purposes only.
(q) pornographic, obscene, or vulgar images, sounds, music, video, language or materials, including screen savers, backdrops, and/or pictures, are prohibited
(r) downloading, uploading, or importing games, screen animations as well as programs or files that can be run or launched
(s) Illegal use or transfer of copyrighted materials to a school-owned computer, including laptops, is prohibited. Students should only download/import music or materials (files) that they are authorized or legally permitted to reproduce, or for which they have the copyright.
(t) File sharing unless District approved.
(u) Adding, modifying or deleting files, except in the student's 'directory' or 'home directory,' are prohibited.
(v) Putting non-school related material (files) on a school file server is prohibited.
(w) Altering/modifying the original District pre-set software image is prohibited. Examples include, but are not limited to:

1. loading/installing any software applications
2. changing the desktop picture
3. changing the computer name
4. changing or removing operating system extensions
5. altering security software
6. altering the pre-loaded operating system or applications
7. taking apart the computer for access to internal parts

Students are expected to report harassment, threats, hate-speech and inappropriate content to a teacher or administrator. If a student has any questions about whether a specific activity is permitted, he or she should ask a teacher or administrator.

(4) Online Assessments

Student assessments may be conducted using technologies such as the Internet or audience response systems. Normally, students will use these technologies as a part of their instructional day. Privacy and security, as defined above, along with confidentiality of assessment responses, are expected.

(5) Vandalism

Any intentional act by a student that damages District technology hardware, software, operating systems, or data will be considered vandalism and will be subject to school rules and disciplinary procedures. Any intentional act that requires a person's time to

repair, replace, or perform corrective work on District technologies or data is also considered vandalism.

(6) Consequences of Misuse

(a) Misuse of personal[2] or District technology resources while on school property, in school vehicles and at school-sponsored activities, as well as the use of District technology resources via off-campus remote access may result in disciplinary action up to and including expulsion.
(b) This regulation shall be used in conjunction with Duluth Public Schools' student policies. In addition, the student's use of District technologies may be suspended or restricted.
(c) A school may temporarily hold (pending parental and/or same-day pick up) personal technology resources that are used inappropriately.
(d) Individual schools may choose to have additional rules and regulations pertaining to the use of personal, networked, and communications resources in their respective buildings.
(e) Intentional unauthorized access and/or damage to networks, servers, user accounts, passwords, or other District resources may be punishable under local, state, or federal law.

(7) Student Access

Parents or guardians who do not wish their children to access the Internet must return the "No Internet Access Form" to their children's schools by the date indicated on the form. These forms will be distributed to all households with the Back-to-School information in August prior to the start of the school year.

The schools' library systems are computerized and are accessed only through the Internet. In addition, the Internet is used extensively for research; and e-mail is accessed through the Internet. If this form is returned, the child's use of Library Media Center resources will be limited to only word-processing, individual computer applications, and other school non-electronic resources.

(8) Student Photographs and Works Displayed on the Internet

Parents or guardians who do not wish their children's pictures or their children's student work to be displayed on the Internet must return the "Student Photographs and Works Displayed on the Internet" form to their children's schools by the date indicated on the form. These forms will be distributed to all households with the Back-to-School information in August prior to the start of the school year.

The Duluth Public Schools may display student pictures and work on the Internet within the following guidelines:

(a) The child may be identified only by first name or nickname, grade, and/or school.
(b) No addresses, telephone numbers or other identifying information may be included in conjunction with a child's name, picture, or work.
(c) If a teacher of child would like to include other information, the teacher must receive written approval from the parent/guardian. No address or telephone numbers can be used even with parent/guardian permission.

B. Appropriate Use of Technology Resources for Staff

Employees of Duluth Public Schools are granted the privilege of using technology only in an authorized and acceptable manner. Generally, a use is unacceptable if it conflicts with Duluth Public Schools or the individual department's purpose, goal, or mission, or interferes with an employee's authorized job duties or responsibilities as determined by his/her immediate supervisor. For purposes of this policy, the term "staff" includes permanent and temporary personnel, substitutes, contract personnel, hourly non-contract personnel, student teachers, volunteers, and outside agency personnel granted use of District technology access.

Administration reserves the right to archive, monitor, review, and audit an employee's use of technology at any time. By using technology, the user consents to this monitoring.

(1) Proper and Acceptable Use of All Technology Resources

Examples of acceptable uses include, but are not limited to, the following types of communication:

(a) for educational purposes;
(b) with students, staff, parents, and other customers of the District;
(c) with federal, state, and local government personnel or agencies, and private businesses with which the School District conducts business;
(d) for professional development;
(e) for administrative purposes;
(f) limited and judicious use of technology for personal use so long as the use is not unacceptable use or violation of School Board policy or the law, and work productivity is not impacted. Employees are to use technology for personal use during designated break time or before/after scheduled work hours;
(g) limited and judicious use of technology for union business. Prior authorization is required from the Department of Human Resources.

Activities that are not permitted when using District or personal technologies include but are not limited to:

(a) excessive personal use of technology. Personal use will be deemed excessive if, in the opinion of an employee's immediate supervisor, the use detracts from the individual employee's or the department's productivity;
(b) communicating to promote personal business ventures (e.g., advertise, promote, or attempt to sell any product, investment, insurance, or other financial proposition) or solicit funds for personal business, political, religious, or other personal causes;
(c) communicating for illegal purposes including, but not limited to: political lobbying, violating copyright laws, using, downloading or copying unauthorized software (including screensavers), creating or knowingly spreading viruses, impersonating another user, or accessing restricted systems;
(d) interfering with or disrupting network users, services, or equipment including, but not limited to: creating or forwarding chain letters, subscribing to any form of personal mailing list; damaging equipment, accessing a system (including using another user id and/or password) without authorization, altering software settings such operating system configurations (except for wallpaper, default colors, and other standard

desktop customization settings), or destroying communications systems or electronic files;

(e) accessing or distributing any communication which may constitute or contain intimidating, hostile, pornographic, offensive or discriminatory material on the basis or sex, race, color, religion, nation origin, sexual orientation or disability;

(f) accessing or participating in news feeds, streaming media (i.e. web radio), "chat" rooms or services (including real time or instantaneous messaging types of services), unless specifically job related.

(2) Consequences of Misuse

(a) Misuse of personal or District technology resources while on school property, in school vehicles and at school-sponsored activities, as well as the use of District technology resources via off-campus remote access may result in disciplinary action up to and including termination.

(b) Intentional unauthorized access and/or damage to networks, servers, user accounts, passwords, or other District resources may be punishable under local, state, or federal law.

C. Privacy and Security

Students and staff must use District technologies responsibly and in a secure manner. They must not share their logins, passwords, or access with others. By using technology, staff is agreeing to, and understands, it is their responsibility to protect employee and/or student information accessed through the Financial/Human Resources information system and/or student information system, and will not release the data to any unauthorized employees or outside agencies.

D. Reliability and Limitation of Liability

(a) The Duluth Public Schools makes no warranties of any kind, expressed or implied, for the technology resources it provides to students and staff.

(b) The Duluth Public Schools will not be responsible for any damages suffered by the student, including those arising from non-deliveries, mis-deliveries, service interruptions, unauthorized use, loss of data, and exposure to potentially harmful or inappropriate material or people. This applies to personal use of technology by staff.

(c) Use of any information obtained via the Internet or communications technologies is at the student's or staff's own risk.

(d) The Duluth Public Schools specifically denies any responsibility for the accuracy or quality of information obtained through the Internet.

(e) The student and his/her parent/guardian will indemnify and hold the Duluth Public Schools harmless from any losses sustained as the result of misuse of the District's technology resources by the student.

[1](Communication systems include e-mail, web sites, cell phones, pagers, text messaging, instant messaging, blogging, podcasting, listserves, and/or other emerging technologies).

[2](Personal technologies include but are not limited to cell phones, digital and image devices, handheld electronic devices, two-way radios, and/or other emerging technologies).

References: MSBA/MASA Model Policy 524

Duluth School District Policy 5085 (School Discipline Policy)
Duluth School District Policy 3090 (Copyright Policy)
Duluth School District Policy 4025 (Standards of Conduct for Personnel)
Duluth School District Policy 3187 (Use Policy for Technology and Internet Access)
Boulder (Colorado) School District Acceptable Internet Use Policy
Henrico (Virginia) County Public Schools Acceptable Use Policy
E-rate Central
Children's Internet Protection Act

Approved: 12-16-97 ISD 709
Revised: 07-21-98
09-21-99
02-15-00
06-19-01
02-19-02
04-20-04
06-12-07
11-20-07
05-13-08