

- Addendum 1 -

ACCEPTABLE USE OF THE DISTRICT'S ELECTRONIC COMMUNICATIONS SYSTEM

• **NORTHSIDE ISD POLICY CQ (LEGAL)** • **NORTHSIDE ISD POLICY CQ (LOCAL)** • **NORTHSIDE ISD ADMINISTRATIVE REGULATION FOR ELECTRONIC COMMUNICATION AND DATA MANAGEMENT**

NORTHSIDE ISD POLICY CQ (LEGAL)

PEIMS

The District shall participate in the Public Education Information Management System (PEIMS) and through that system shall provide information required for the administration of the Foundation School Program and of other appropriate provisions of the Education Code. The PEIMS data standards, established by the Commissioner of Education, shall be used by the District to submit information. *Education Code 42.006; 19 TAC 61.1025*

CHILDREN'S INTERNET PROTECTION ACT

Under the Children's Internet Protection Act (CIPA), the District must, as a prerequisite to receiving universal service discount rates, implement certain Internet safety measures and submit certification to the Federal Communications Commission (FCC). *47 U.S.C. 254* [See UNIVERSAL SERVICE DISCOUNTS, below, for details]

Districts that do not receive universal service discounts but do receive funding under the Technology for Education Act of 1994 (Title III of the Elementary and Secondary Education Act [ESEA]) must, as a prerequisite to receiving these funds, implement certain Internet safety measures and submit certification to the Department of Education (DOE). *20 U.S.C. 7001* [See ESEA FUNDING, below, for details]

DEFINITIONS

"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;
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.

47 U.S.C. 254(h)(7)(G), 20 U.S.C. 7001(a)(5)(F)

"Technology protection measure" means a specific technology that blocks or filters Internet access. *47 U.S.C. 254(h)(7)*

"Universal service" means telecommunications services including Internet access, Internet services, and internal connection services and other services that are identified by the FCC as eligible for federal universal service support mechanisms. *47 U.S.C. 254(c)(3), (h)(5)(A)(ii)*

UNIVERSAL SERVICE DISCOUNTS

An elementary or secondary school having computers with Internet access may not receive universal service discount rates unless the District implements an Internet safety policy, submits certifications to the FCC, and ensures the use of computers with Internet access in accordance with the certifications. *47 U.S.C. 254(h)(5)(A), (I); 47 CFR 54.520*

INTERNET SAFETY POLICY

The District shall adopt and implement an Internet safety policy that addresses:

1. Access by minors to inappropriate matter on the Internet and the World Wide Web;

2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including "hacking," and other unlawful activities by minors on-line;
4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
5. Measures designed to restrict minors' access to materials harmful to minors.

47 U.S.C. 254(l)

PUBLIC HEARING

The District shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy. *47 U.S.C. 254(h)(5)(A), (l)(1)*

INAPPROPRIATE FOR MINORS

A determination regarding what matter is inappropriate for minors shall be made by the Board or designee. *47 U.S.C. 254(l)(2)*

TECHNOLOGY PROTECTION MEASURE

In accordance with the appropriate certification, the District shall operate a technology protection measure that protects minors against access to visual depictions that are obscene, child pornography, or harmful to minors; and protects adults against access to visual depictions that are obscene or child pornography. *47 U.S.C. 254(h)(5)(B), (C)*

MONITORED USE

In accordance with the appropriate certification, the District shall monitor the on-line activities of minors. *47 U.S.C. 254(h)(5)(B)*

CERTIFICATIONS TO THE FCC

To be eligible for universal service discount rates, the District shall certify to the FCC, in the manner prescribed at *47 CFR 54.520*, that:

1. An Internet safety policy has been adopted and implemented.
2. With respect to use by minors, the District is enforcing the Internet safety policy and operating a technology protection measure during any use of the computers.
3. With respect to use by adults, the District is enforcing an Internet safety policy and operating a technology protection measure during any use of the computers, except that an administrator, supervisor, or other person authorized by the District may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose.

47 U.S.C. 254(h)(5); 47 CFR 54.520

ESEA FUNDING

Federal funds made available under the Technology for Education Act of 1994 (Title III of the Elementary and Secondary Education Act [ESEA]) for an elementary or secondary school that does not receive universal service discount rates may not be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet unless the District:

Minors

1. Has in place a policy of Internet safety for minors that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and enforces the operation of the technology protection measure during any use by minors of its computers with Internet access; and

Adults

2. Has in place a policy of Internet safety that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene or child pornography; and enforces the operation of the technology protection measure during any use of its computers with Internet access. The District may disable the technology protection measure to enable access to bona fide research or for another lawful purpose.

CERTIFICATION TO DOE

The District shall certify its compliance with these requirements to the Department of Education as part of the annual application process for each program funding year under the ESEA.

20 U.S.C. 7001(a)

TRANSFER OF EQUIPMENT TO STUDENTS

The District may transfer to a student enrolled in the District:

1. Any data processing equipment donated to the District, including equipment donated by a private donor, a state eleemosynary institution, or a state agency under Government Code 2175.126;
2. Any equipment purchased by the District; and
3. Any surplus or salvage equipment owned by the District.

Education Code 32.102(a)

Before transferring data processing equipment to a student, the District must:

1. Adopt rules governing transfers, including provisions for technical assistance to the student by the District;
2. Determine that the transfer serves a public purpose and benefits the District; and
3. Remove from the equipment any offensive, confidential, or proprietary information, as determined by the District.

Education Code 32.104

DONATIONS

The District may accept:

1. Donations of data processing equipment for transfer to students; and
2. Gifts, grants, or donations of money or services to purchase, refurbish, or repair data processing equipment.

Education Code 32.102(b)

USE OF PUBLIC FUNDS

The District may spend public funds to:

1. Purchase, refurbish, or repair any data processing equipment transferred to a student; and
2. Store, transport, or transfer data processing equipment under this policy.

Education Code 32.105

ELIGIBILITY

A student is eligible to receive data processing equipment under this policy only if the student does not otherwise have home access to data processing equipment, as determined by the District. The District shall give preference to educationally disadvantaged students. *Education Code 32.103*

RETURN OF EQUIPMENT

Except as provided below, a student who receives data processing equipment from the District under this policy shall return the equipment to the District not later than the earliest of:

1. Five years after the date the student receives the equipment;
2. The date the student graduates;
3. The date the student transfers to another district; or
4. The date the student withdraws from school.

If, at the time the student is required to return the equipment, the District determines that the equipment has no marketable value, the student is not required to return the equipment.

Education Code 32.106

UNIFORM ELECTRONIC TRANSACTIONS ACT

The District may agree with other parties to conduct transactions by electronic means. Any such agreement or transaction must be done in accordance with the Uniform Electronic Transactions Act. *Business and Commerce Code 43.*

NORTHSIDE ISD POLICY CQ (LOCAL)

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

AVAILABILITY OF ACCESS

Access to the District's computers, the electronic communications system, the Internet, and other computer resources shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

USE BY MEMBERS OF THE PUBLIC

When possible and available and in accordance with the District's administrative regulations, members of the District community may use the District's computers, including the electronic communications systems, the Internet, other computer resources, and software for education or District-related activities, but only if the primary mission of technology for students and staff is not hampered and if no substantial financial impact is anticipated. The equipment, software, and network resources provided through the District are and remain the property of the District. Users of District equipment shall comply with all policies, procedures, and guidelines of the District and access may be denied to any student, employee, or community member who fails to comply with those policies, procedures, and guidelines.

ACCEPTABLE USE

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy.

Access to District computers, the electronic communications system, the Internet, and other computer resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all policies and administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with these policies, regulations, and guidelines. Non-compliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

PERSONAL SOFTWARE

Personal software may not be loaded on District computers.

DISTRICT SOFTWARE

All software used in District computers must be legally licensed. Proper documentation must be maintained.

INTERNET SAFETY

The Superintendent or designee shall develop and implement an Internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities; and

4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.

FILTERING

Each District computer with Internet access shall have a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

The Superintendent or designee shall enforce the use of such filtering devices. Upon approval from the Superintendent or designee, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.

MONITORED USE

The District reserves the right to monitor access to and use of e-mail, the Internet, or other network or computer-related activity, engage in routine computer maintenance and housekeeping, carry out internal investigations, prepare responses to requests for public records, or disclose messages, data, or files to law enforcement authorities. Monitoring shall be restricted to individuals specifically designated by the Superintendent.

INTELLECTUAL PROPERTY RIGHTS

Students shall retain all rights to work they create using the District's electronic communications system.

As agents of the District, employees shall have limited rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created in the scope of a person's employment even when the author is no longer an employee of the District.

ELECTRONIC COPYRIGHT LAW

The electronic transmission, distribution, or use of copyrighted materials through the District's electronic communications system beyond Fair Use without required citation or written permission by the author is prohibited.

DISCLAIMER OF LIABILITY

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

This presentation of your district's policy is a representation of TASB's record of the district's currently adopted policy manual. It does not reflect updating activities in progress. The official, authoritative manual is available for inspection in the office of the Superintendent. [See BF (LOCAL) for further information.]

NORTHSIDE ISD ADMINISTRATIVE REGULATION FOR ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

The Superintendent or designee will oversee the District's electronic communications system.

The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical and safe use of this resource.

CONSENT REQUIREMENTS

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the copyright owner, or an individual the owner specifically authorizes, may upload copyrighted material to the system.

No original work created by any District student or employee will be posted on a

Web page under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor) or employee who created the work. [See CQ(EXHIBIT)]

No personally identifiable information about a District student will be posted on a Web page under the District's control unless the District has received written consent from the student's parent.

FILTERING

The Superintendent will appoint a committee, to be chaired by the Deputy Superintendent for Instruction, to select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers with Internet access provided by the school.

The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to: nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and on-line gambling.

REQUESTS TO DISABLE FILTER

The committee will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes. The committee will make recommendation to the Superintendent or designee regarding approval or disapproval of disabling the filter for the requested use.

SYSTEM ACCESS

Access to the District's electronic communications system will be governed as follows:

1. Students in all grades will be granted access to the District's system, as appropriate. Students may be assigned individual accounts, as appropriate.
2. As appropriate, District employees will be granted access to the District's system.
3. A teacher may apply for a class account and, in doing so, will be ultimately responsible for use of the account.
4. The District will require that all passwords be changed on a regular basis.
5. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system.
6. All users will be required to sign a user agreement annually for issuance or renewal of an account. (See 2 below)

TECHNOLOGY SUPERVISION RESPONSIBILITIES

The Superintendent or designees will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.
2. Ensure that all users of the District's system annually complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or supervisor's office.
3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure student online safety and proper use of the system.
6. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose, with approval from the Superintendent.
7. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.
8. Set limits for data storage within the District's system, as needed.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's electronic information/communications systems:

ON-LINE CONDUCT

1. The individual in whose name a system account is issued will be responsible at all times for its proper use. Passwords and other information related to system and network access are restricted to that individual and must not be shared with anyone else.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
3. System users may not disable, or attempt to disable, a filtering device on the District's electronic communications system.
4. Communications may not be encrypted so as to avoid security review by system administrators.
5. System users may not use another person's system account without written permission from a supervising administrator or the Executive Director for Information and Technology Services, as appropriate.
6. Students may not distribute personal information about themselves or others by means of the electronic communications system; this includes, but is not limited to, personal addresses and telephone numbers.
7. Students should never make appointments to meet people whom they meet online and should report to a teacher or administrator if they receive any request for such a meeting.
8. System users must purge electronic mail in accordance with established retention guidelines.
9. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
10. System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages from unknown senders and loading data from unprotected computers.
11. System users may upload or download District approved public domain programs to the system.. The District will maintain an electronic list of approved public domain programs.
12. System users may not send, forward or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
13. Users may not send, forward, or post chain e-mail or other messages that are personal for-profit use.
14. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
15. System users may not misrepresent the District through electronic communication. They should be mindful that use of school-related electronic mail addresses and fax transmissions might cause some recipients or other readers of that communication to assume they represent the District or school, whether or not that was the user's intention.
16. System users may not abuse or waste District electronic communications system resources (e.g. e-mail spamming, mass distribution of videos, photos, etc.)
17. System users may not gain unauthorized access to resources or information.
18. District email broadcasts must be approved by the Director of Communications.

VANDALISM PROHIBITED

Any attempt to harm or destroy District equipment or data or the data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading, downloading or creating of computer viruses or hacking tools.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences. [See DH, FN series, FO series, and the Student Code of Conduct]

FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages and signatures is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

INFORMATION CONTENT / THIRD-PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that, despite the District's use of technology protection measures as required by law, use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]

PARTICIPATION IN CHAT ROOMS AND NEWSGROUPS

Participation in chat rooms and newsgroups accessed on the Internet is permissible for students, under appropriate supervision, and for employees. Use will be limited to educational and District related activities.

DISTRICT WEB SITE

The District will maintain a District Web site for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District Web site must be directed to the designated Webmaster. The Director of Communications and the Coordinator of Web Information, in collaboration with the technology departments, will establish guidelines for the development and format of Web pages controlled by the District. Campus web pages will be linked to the District Web site by the Coordinator of Web Information.

No personally identifiable information regarding a student will be published on a Web site controlled by the District without written permission from the student's parent.

No commercial advertising will be permitted on a Web site controlled by the District.

SCHOOL OR CLASS WEB PAGES

Schools or classes may publish and link web pages to the campus Web pages that present information about the school or class activities, subject to approval from the campus principal or designee (campus Webmaster). The campus principal will designate the staff member responsible for managing the campus's Web page. Teachers will be responsible for compliance with District rules in maintaining their class Web pages. Any links from a school or class Web page to sites outside the District's computer network must receive approval from the campus principal or designee.

STUDENT WEB PAGES

With the approval of the campus principal or designee, students may submit individual Web pages to be linked to campus Web pages. All material presented on a student's Web page must be related to the student's educational activities and must conform to the District Acceptable Use Policies. Student Web pages must include the following notice: "This is a student Web page. Opinions expressed on this page shall not be attributed to the District." Any links from a student's Web page to sites outside the District's computer system must receive approval from the campus principal or designee.

EXTRA-CURRICULAR ORGANIZATION WEB PAGES

With the approval of the campus principal, campus extracurricular organizations may submit Web pages to be linked to that campus' Web site. All material presented on the Web page must relate specifically to organization activities and include only staff or student-produced material. The web page must conform to the District Acceptable Use Policies. The sponsor of the organization will be responsible for compliance with District web development and maintenance rules. Web pages of extracurricular organizations must include the following notice: "This is a student extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the District ." Any links from the Web page of an extracurricular organization to sites outside the District's computer system must receive approval from the campus principal or designee.

PERSONAL WEB PAGES

District employees, Trustees, and members of the public will not be permitted to publish personal Web pages using District resources.

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is considered inappropriate.
4. Transmitting obscene messages or pictures is prohibited.
5. Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the recipient's system or may be in a format unreadable by the recipient.
6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

TERMINATION / REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the principal or District supervisor issues/receives notice of revocation of system privileges, or on a future date if so specified in the notice.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.