NORTHWEST INDEPENDENT SCHOOL DISTRICT
STUDENT GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES

Acceptable Use for Technology Resources

The Northwest Independent School District ("Northwest ISD", "NISD", or the "District") provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence within Northwest ISD by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff. The use of these technology resources is a privilege, not a right.

With access to many different technology resources and people from all over the world, there comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Northwest ISD firmly believes that the value of information, interaction, and research capabilities available (including, but not limited to, e-mail, the Internet, and social media) outweighs the possibility that users may obtain material that is not consistent with the educational goals of the District. Access to the District's electronic communication and data management systems, including without limit its telephone system, software, hardware, technology resources, computer networks, electronic mail systems, video conferencing systems, and its Internet and Intranet access capabilities (collectively referred to herein as the "System") shall be made available to students for education and administrative purposes that are consistent with the goals and mission of the District.

Proper behavior, as it relates to the use of the System, is no different than proper behavior in all other aspects of Northwest ISD activities. All users are expected to use the System in a responsible, ethical, polite manner, and in accordance with NISD Board of Trustees' Policies. This document is intended to clarify those expectations as they apply to technology resource usage and is consistent with District policy.

These guidelines are provided so that students and parents are aware of the responsibilities students accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communication technologies, social media resources, Internet access, electronic communication, and electronic equipment provided by the District. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations are as follows:

a. The District's technology resources will be used by students for learning purposes consistent with the District's mission and goals.

b. Student use of the System is only allowed when supervised or granted permission by a staff member.

c. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the libraries of each campus as well as posted on the District's website.

d. Although the District has an Internet safety plan in place, students are expected to notify a teacher or principal whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

e. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.

f. Students are responsible for the proper handling and care of technology devices and returning them in good working conditions.

2. Unacceptable conduct includes, but is not limited to, the following:

a. Using the System for illegal activities, including copyright, license, or contract violations or downloading inappropriate materials, viruses, and/or software, such as, but not limited to, hacking and host file-sharing software.

b. Possessing, accessing, transmitting, copying, or creating material that violates the *Student Handbook and Code of Conduct,* District policy, or District rules and regulations, including but not limited to content that is inappropriate, illegal, copyrighted, pornographic or obscene, stolen, threatening, discriminatory, harassing, or offensive.

c. Attempting to bypass or disable the District's Internet filter, security systems, or software.

d. Attempting to access or install unlicensed, inappropriate, or unapproved software or technology.

e. Plagiarizing or using of District technology resources to engage in academic dishonesty.

f. Using the network for financial or commercial gain, advertising, or political lobbying.

g. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as, but not limited to, pornographic sites.

h. Vandalizing and/or tampering with the System. Use or possession of hacking software is strictly prohibited.

i. Unauthorized use of the System and/or any District technology resource or personal/NISD device for non-educational purposes or outside the bounds of NISD curriculum.

j. Causing congestion on the System or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.

k. Intentionally wasting finite System resources (i.e., intentionally accessing an online service where the District only has a finite number of hours of use and leaving the computer logged onto the service while no longer using the online service).

l. Gaining unauthorized access anywhere on the System.

m. Revealing the home address or phone number of one's self or another person, unless done upon the prior request of the District.

n. Invading the privacy of other individuals.

o. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.

p. Coaching, helping, observing, or joining any unauthorized activity on the System.

q. Posting anonymous messages or unlawful information on the System.

r. Engaging in sexual harassment or submitting, publishing, or displaying any inaccurate, racially and/or culturally offensive, sexually offensive, sexually oriented, abusive, obscene, profane, threatening, terroristic, demeaning, stalking, or slanderous messages, whether public or private.

s. Falsifying permission, authorization, or identification documents.

t. Obtaining copies of or modifying files, data, or passwords belonging to other users on the System.

u. Attempting to upload, create, or transmit a computer virus on a computer or the System.

v. Using e-mail, the Internet, or social media resources at school to encourage illegal behavior, engage in conduct that is in conflict or violates the *Student Handbook and Student Code of Conduct*, or threaten school safety.

w. Using personal e-mail, the Internet, the System, or social media resources, without regard to whether it occurs on school property, to engage in conduct that involves a public school and contains the elements of the offense of terroristic threat or false alarm, or otherwise causes a substantial disruption to the educational environment.

x. Downloading software on the System or any system connected to the District's System without prior permission from District.

y. Placing any copyrighted software or data on the District's System or any system connected to the District's System without prior permission from holder of the copyright. Only the copyright owner or individual the owner specifically authorizes may upload copyrighted materials to the System.

3. Acceptable use guidelines for the System's computer online services are as follows:

a. General Guidelines:

(1) Students will have access to available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.

(2) Students are responsible for their ethical and educational use of the System.

(3) All policies and restrictions of the System must be followed.

(4) Access to the System is a privilege and not a right. Each student and/or parent will be required to sign the Student Guidelines Acceptable Use of Technology Resources Agreement and adhere to these Guidelines in order to be granted access to the System.

(5) The use of any District computer online services in the District must be in support of education and research and in support of the educational goals and objectives of the District.

(6) When placing, removing, or restricting access to specific databases or other District computer online services, school officials will apply the same criteria of educational suitability used for other education resources.

(7) Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to, confidential information, copyrighted material, threatening or obscene material, and computer viruses.

(8) Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the District's *Student Handbook and Code of Conduct* and District policy.

(9) Parents concerned with the District's computer online services at their child's school should refer to EFA (LOCAL): Instructional Resources: Instructional Material Selection and Adoption policy and follow the stated procedure.

(10) Parents will assume responsibility for imposing restrictions only on their own children.

b. System Etiquette:

All System users are expected to observe the following System etiquette:

(1) Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.

(2) Pretending to be someone else when sending/receiving messages is prohibited.

(3) Submitting, publishing, or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented or threatening materials or messages either public or private is prohibited.

(4) Transmitting obscene messages or pictures is prohibited.

(5) Revealing and/or posting any personally identifiable information such as addresses, phone numbers, or photographs of another individual on any website or social media network, is prohibited unless the student reveals and/or posts such personal information in compliance with all school poli-

cies and under the supervision and consent of a teacher and/or administrator. Other restrictions apply to revealing and/or posting personally identifiable information about other students. (see (3)(b)(7) below)

(6) Using the network in such a way that would disrupt the use of the network by other users is prohibited.

(7) Revealing and/or posting any personally identifiable information, including photographs, of another student on any website or social media network, including the District's website, is prohibited unless (a) such information is directory information; (b) the directory information privacy code specified for the student allows it as recorded in eSchool Plus; (c) the release and/or posting of such personal information is in compliance with District policy FL (LEGAL); and (d) the release and/or posting of such personal information is under the supervision of a teacher and/or administrator.

c. Monitored Use and No Right to Privacy:

(1) Electronic mail transmissions and other use of the System by students are not private and may be monitored, reviewed, audited, intercepted, accessed, or disclosed at any time by designated District staff to ensure appropriate use, ensure the safety and integrity of the System, diagnose problems, and investigate reports of illegal or impermissible activities.

(2) Users should be aware that the District will comply with lawful orders of courts, such as subpoenas and search warrants. The District is also subject to the Texas Public Information Act which may require disclosure of information transmitted through its System, including e-mail communications.

d. E-Mail:

(1) E-mail should be used for educational purposes only.

(2) E-mail transmissions, stored data, transmitted data, or any other use of the System by students, employees, or any other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

(3) All e-mail and all e-mail content are property of the District.

(4) E-mails should only be forwarded by a student to another person that would need the information contained in the e-mail for educational or administrative purposes that are consistent with the goals and mission of the District.

(5) Never assume electronic mail is private. Messages relating to or in support of illegal activities must be reported to the authorities and the District will comply with state and federal laws, as well as court orders or subpoenas that will require disclosure.

(6) Be brief and professional: Few people will bother to read a long message or one that is not narrowly tailored to the underlying purpose of the communications.

(7) Include your signature (name, position, affiliation, and Internet address) at the bottom of e-mail messages.

(8) Send only to individuals and/or groups you know.

e. Blogs, Podcasts, Social Networking, and Wikis:

(1) Only student or teacher-created blogs or podcasts related to and in support of the District-approved curriculum and in compliance with all District policies may be posted using the System. Use of the System to post personal blogs, forums, wikis, or podcasts is prohibited.

(2) Participation in social networking websites or chat rooms for educational purposes is permissible for students, under the supervision of a District's teacher, librarian, or administrator.

(3) Students participating in social networking websites or chat rooms using District electronic resources should assume that all content shared, including pictures, is public. Students should not respond to requests for personally identifying information or contact unknown individuals. Caution should be taken when addressing questions that would violate FERPA (Family Education Rights and Privacy Act) or student information. No student shall post on a website personally identifiable information, including photographs, of himself/herself or any other student. (See 3 (b) (5) and 3 (b) (7).)

(4) Posting any student or teacher created podcast and/or blog projects that are not directly related to and in support of the NISD approved curriculum is prohibited.

(5) Posting of any unsupervised student blog is prohibited.

f. Display of Student Work or Information:

The following conditions apply to the display of student work including, but not limited to art work, class work, photographs, podcasts, projects, and writings on the District's websites or other Internet sites. Student work that has been recorded for a grade is considered an "educational record."

(1) All student work or photographs to be displayed must follow the standards for the "Limitations on Content" as sited in NISD Local policies FNAA and GKDA, and when applicable, must be compliant with the dress code as described in the *NISD Student Handbook and Code of Conduct*.

(2) Parental consent for students under the age of 18 must be obtained prior to posting student-created work on campus and/or District websites, social networking, and/or other Internet sites (See 3 (b) (5) and 3 (b) (7).)

(3) Students may not transmit pictures without obtaining prior permission from all individuals depicted, or from parents of depicted individuals who are under the age of 18.

(4) Student photographs and/or student work may only be displayed with directory information for which the directory information privacy code specified for the student allows it as recorded in eSchool Plus.

g. Hyperlinks:

The following requirements must be met to utilize hyperlinks on any District web page. If these conditions are not met, or promotes the violation of any District policy, regulation, or any local, state, or federal regulation or law, immediate disciplinary action of the individual responsible for the content, file, and/or posting of the hyperlink may be recommended.

(1) Hyperlinks to external (non-District) websites must include the following text on the District web page where the hyperlink exists: “Northwest ISD is not responsible for content on external sites or servers.”

(2) Hyperlinks to external (non-District) websites are only allowed where the content in those websites support and/or enhance learning, academic knowledge, and/or provide information necessary to provide service to District web patrons. However, if the content in these websites is judged unsuitable at any time, the hyperlink to the site will be removed.

(3) Hyperlinks to websites, whose content is prohibited by the District’s web filtering system, will not be allowed.

(4) Hyperlinks to District employee, volunteer, or student personal websites are not allowed.

h. Filtering and Requests to Disable Filter:

The District will use filtering devices or software that blocks Internet access to visual depictions that are obscene, violent, 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.

(1) Internet filters may be disabled for employees based on a Tiered Access System.

(2) Employees may request to use a blocked Internet site for research, or other educational or lawful purposes. Students may have the opportunity to view District-approved disabled blocked Internet sites under the supervision of a staff member as it relates to the instruction.

(3) Students will not have the authority to request Internet filters to be disabled.

4. Intellectual Property Rights:

a. Students shall retain all rights to work they create using the System.

5. Reporting Theft or Releasing Resources:

a. Electronic resources owned by the District should not be released to anyone, including but not limited to, law enforcement agencies. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the Texas Public Information Act; therefore, proper authorities will be given access to their content.

b. Report theft or loss to the School Resource Officers (SRO) within 48 hours. If the incident occurs on the weekend or school holiday, a report must be filed upon 48 hours of returning to school. Failure to report the theft or loss will result in the parent or guardian, or a student 18 years or older, being held responsible for the replacement of the netbook at fair market value.

6. Consequences of improper use are as follows:

a. The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use. Noncompliance with the *Student Guidelines for Acceptable Use of Technology Resources*, the *Student Handbook and Code of Conduct*, and Board policy CQ may result in suspension or termination of System privileges and disciplinary actions. This may also require restitution for costs associated with the necessary repairs and/or replacement of system, hardware, or software if any damage was caused by student's noncompliance or improper use of District's System.

b. Use or possession of hacking software is strictly prohibited and violators will be subject to Phase III consequences of the *Student Handbook and Code of Conduct.*

c. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, Chapter 33, will result in criminal prosecution, as well as disciplinary actions by the District.

d. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the Texas Public Information Act; therefore, proper authorities will be given access to their content.

7. Disclaimer:

The District's System is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including without limitation, those of merchantability and fitness for 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.