NORTHWEST INDEPENDENT SCHOOL DISTRICT

EMPLOYEE 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 primarily 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 employees 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 from 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 the district's board 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 employees are aware of the responsibilities employees 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 primarily for learning, teaching, and administrative purposes consistent with the district's mission and goals, but some limited personal use is permitted.

   b. The employee shall limit personal electronic communication devices to send or receive calls, text messages, pictures, and videos to breaks, meal times, and before and after scheduled work hours, unless there is an emergency or the use is authorized by a supervisor to conduct district business.

   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, employees are expected to notify their supervisor or the assistant superintendent for curriculum and instruction or designee whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

   e. Employees who identify or know about a security problem are expected to convey the details to their supervisor or the chief technology officer or designee without discussing it with others.

   f. Employees are responsible for securing technology devices when not in use and for returning them in good working conditions.

g. District employees are considered public servants. The online presence of employees should not be in conflict with board policies or the district's Acceptable Use Guidelines for Technology Resources.

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

a. Use of the System for a purpose other than for learning, teaching, and/or administrative purposes consistent with the district's mission and goals or not in accordance with CQ legal and local policy.

b. 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.

c. Using the System for financial or commercial gain, advertising, or political lobbying.

d. Attempting to bypass or disable the district's Internet filter, security systems or software.

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

f. Plagiarizing or using district technology resources to engage in academic dishonesty.

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 equipment, programs, files, software, System performance, or other components of the System. Use or possession of hacking software is strictly prohibited.

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

j. Intentionally wasting 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).

k. Gaining unauthorized access anywhere on the System.

l. Revealing the home address or phone number of another person, unless done upon the prior request of the district.

m. Invading the privacy of other individuals.

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

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

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

q. 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.

r. Falsifying permission, authorization, or identification documents.

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

t. Attempting to upload, create, or transmit a computer virus on a computer and/or the System.

u. Using e-mail, the Internet, or social media resources at school to encourage illegal behavior, engage in conduct violates the *Educator Code or Ethics* (NISD Local Policy DH and Exhibit DH), or threaten school safety.

v. Using personal e-mail, the Internet, 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.

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

x. Knowingly communicate with students through a personal social network system in violation of the NISD employee handbook, administrative regulations, *Educator Code or Ethics* (NISD Local Policy DH and Exhibit DH) and CQ legal and local policy.

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

a. General Guidelines:

(1) Employees will have access to all available forms of electronic media and communication that is in support of learning, teaching, and/or administration, and in support of the educational goals and objectives of the district.

(2) Employees are responsible for their ethical and educational use of the System in the District.

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

(4) Access to the System is a privilege and not a right. Each employee, will be required to sign the *Employee 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 System must be in support of education and research and in support of the educational goals of the district in accordance with CQ legal and local policy.

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

(9) Employees must purge electronic mail and data files in accordance with the District's established retention guidelines.

a. 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, whether 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 employee reveals and/or posts such personal information in compliance with all school policies. Other restrictions apply to revealing and/or posting personally identifiable information about students. (See (3) (b) (7) below.)

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

(7) Revealing and/or posting any personally identifiable information, including photographs, of any 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).

b. Monitored Use and No Right to Privacy:

(1) Electronic mail transmissions and other use of the System by employees 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.

c. E-Mail:

(1) E-mail should be used primarily for educational and administrative purposes.

(2) E-mail transmissions, stored data, transmitted data, or any other use of the System by 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 contents are property of the district.

(4) E-mails may only be forwarded by an employee only if such e-mail is forwarded to a person who 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) An employee must include his/her signature (name, position, affiliation, and Internet address) at the bottom of e-mail messages.

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

(1) Only students 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 must be in accordance with CQ legal and local policy.

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

(3) Employees participating in social networking websites and chat rooms using District electronic resources should assume that all content shared, including pictures, is public. Employees 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 employee shall post personally identifiable information, including photographs, of a student on any website, including the district's website without parental consent. (See (3) (b) (5) and (3) (b) (7).)

(4) Posting any student- or teacher-created podcast and/or blog projects that are not in support of the NISD vision, mission, and goals is prohibited.

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

e. 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, is compliant with the dress code as described in the *NISD Student Handbook and Student 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) Employees 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 allow 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 filtering may be disabled for employees based on a Tiered Access System that is available on the district's website.

(2) Employees may request to use a blocked site for research, or other educational or lawful purposes. The request must be filed with and approved by the chief technology officer or designee.

4. Intellectual Property Rights:

a. The district will own any work or work product created by an employee using the system, including a student employee, if it is in the course and scope of the employee's employment, including the right to obtain copyrights.

b. The District will 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.

c. An employee who obtains a patent for such work shall grant a non-exclusive, non-transferable, perpetual, royalty-free district-wide license to the district for use of the patented work.

d. A student will retain all rights to work created as part of instruction or using district technology resources.

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.

b. Report theft or loss to the district's personnel and risk management office within 48 hours, if possible. If the incident occurs on the weekend or school holiday, please attempt to report the theft or loss upon 48 hours of returning to school. A copy of the police report should accompany the theft or loss claim.

6. Consequences of improper use are as follows:

a. The employee in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use.

b. Noncompliance with the *Employee Guidelines for Acceptable Use of Technology Resources* and in Board policy CQ may result in suspension or termination of System privileges and disciplinary actions. Violations of applicable state and federal law, including the Texas Penal Code, Computer

Crimes, and Chapter 33 will result in criminal prosecution, as well as disciplinary actions by the District. 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 noncompliance.

c. 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 expressed 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 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, and federal officials in any investigation concerning or relating to misuse of the District's electronic communications System.