

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

Introduction and Purpose of this Document

Northwest ISD understands that leveraging technology, both in the classroom and at home, provides the opportunity for students to become progressively active learners, problem-solvers and creative thinkers. In order to accomplish the future ready vision, Northwest ISD embraces what it means to be a future ready learner by engaging our students in safe, ethical practices in a digital environment. The Responsible Use Policy is based on the premise that future ready students need to learn how to be responsible users, make informed choices and exercise accountability for their behavior. When using the System and technology devices, student behavior should reflect the same responsible, ethical behavior as outlined in the Student Code of Conduct. This document is intended to provide clarification on those expectations as they apply to technology usage and is consistent with District policy.

Annual Review

Students are required to review these guidelines at the beginning of each school year and agree to the terms in writing. The parent or legal guardian of a student user is required to acknowledge receipt and understanding of the District's Student Responsible Use Guidelines for Technology as part of their review of the Student/Parent Handbook and the Student Code of Conduct.

Digital Citizens of Northwest ISD

Students using technology resources should practice appropriate digital citizenship. All information transmitted digitally is public and permanent. Appropriate digital citizenship includes:

Respecting Yourself. Users will apply appropriate language/content in all online posts, as users continuously represent Northwest ISD and yourself whenever and wherever they use online communications.

Protecting Yourself. Users will not publish personally identifiable information or data for themselves or anyone else. Users are the custodian of their accounts and are responsible for all activity initiated by and/or performed under their accounts. It is the responsibility of each user to appropriately secure account credentials (user IDs/passwords) and to maintain and backup all of their data. If a user is uncertain whether a specific computer activity is permitted or appropriate, he/she should ask a teacher/administrator before engaging in the activity. (This includes passwords.)

Respecting Others. Users will not use technology resources to bully, harass or tease other people. Users will not make an audio or video recording of any student, teacher, or administrator without prior permission from the subject. No user will pose as someone else, or pose as a user other than him or herself when online. Users will not access, download, or modify accounts, files, or data belonging to others. Users will adhere to current copyright law.

Protecting Others. Users will help maintain a safe computing environment by notifying appropriate campus officials of inappropriate behavior, online bullying or harassment, vulnerabilities, risks, and breaches involving campus technology.

Respecting and Protecting Intellectual Property. Users will adequately cite any and all websites, books, media, etc. used in creating homework or other school projects. Users will respect all copyrights, requesting permission for the use of software, media, and the intellectual property of others.

Monitoring of Computer and Internet Usage

Users should have no expectation of privacy regarding their use of District property and technology resources. In general, communications or transmissions made through technology resources should never be considered private or confidential. The District reserves the right to monitor the use of its network and all technology resources as it deems necessary to ensure the safety and integrity of its network, diagnose problems, investigate reports of illegal or impermissible activity, and ensure user compliance with state and federal laws and the District's policies. In addition, 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 technology resources, including e-mail communications.

Children's Online Privacy Protection Act (COPPA)

For students under the age of 13, the Children's Online Privacy Protection Act (COPPA) requires additional parental permission for educational software tools. Parents wishing to deny access to these educational tools must do so in writing to the campus principal indicating their child should be denied access to these tools. Examples of these tools are Google Suite for Education, blogs, online presentation tools, and other digital resources.

Bring Your Own Device (BYOD)

NISD permits students to bring their own device for use during the school day and connect to the guest network. This Internet access is filtered by the District on personal technology devices in the same manner as District-owned equipment. If network access is needed, connection to the filtered, wireless network provided by the District is required. BYOD devices are the sole responsibility of the student owner. The campus or District assumes no responsibility for personal technology devices if they are lost, loaned, damaged or stolen. Students are prohibited from trading or selling these items to other students on District property, including school buses. Each student is responsible for his/her own device: setup, maintenance, charging, and security. Campus administrators and staff members have the right to prohibit use of BYOD devices at certain times, during designated activities (i.e. campus presentations, theatrical performances, or guest speakers) or designated locations (restrooms and locker rooms) while students are on campus. An administrator may examine a student's personal technology device and search its contents, in accordance with disciplinary guidelines. For a list of FAQs regarding the District's BYOD policy, visit the District's website.

Use of District Provided Internet Access

The District's goal is to increase student access to digital tools and facilitate immediate access to technology-based information including textbooks, teacher built content, and other digital materials. The District will utilize a filtered, wireless network as defined by the federal Children's Internet Protection Act (CIPA) through which all student devices will connect. Any attempt to disable or circumvent (aka proxy) the District filter is strictly prohibited. Students will be allowed

to use the Internet between classes and in the cafeteria setting at the discretion of campus leadership. Causing network congestion through mass consumption of system resources is prohibited. Examples of this include extensive video or game streaming and mass email forwards.

Student Access to District Devices

Computer/Network/Internet access is provided to all students unless parents or guardians request in writing to the campus principal that access be denied. Students may also be allowed to use the local network and public Wi-Fi with campus permission. For access to a 1:1 device, parents of secondary students must fill out the *1:1 Secondary Student Device Usage Agreement Form* prior to receiving the student device.

Access for All Students

The District is committed to ensuring that all students can access the educational opportunities and benefits available through District devices and web content. If a device or opportunity is not equally accessible to a student, the student or parents should contact the campus principal so accommodations or modifications can be provided, as needed.

Appropriate Behavior

Access to the District's computer/network/Internet is a privilege, not a right. Campus and District Administrators are responsible for determining what is considered to be inappropriate use of the Northwest ISD computer network. They may request to disable a user's account or network access at any time. Student discipline will be referred to campus administration, while staff behavior will be referred to the employee's supervisor and Human Resources. All actions on a district issued device may be monitored at any time. Both District issued and personal technology devices are subject to examination in accordance with disciplinary guidelines if there is reason to believe that the Responsible Use Guidelines have been violated.

Physical Care of Property

- Keep the device secure and damage free.
- Keep track of your device, charger, and cord.
- Bring your charged device to school each day.
- Make sure to store your device in a secure environment when not in use. Some examples of unsecure locations are: car, unlocked athletic locker, bleachers, etc.
- Devices are not water resistant. Take precautions when dealing with liquids and food.
- Devices are not intended to have heavy weight placed on them. Do not stack things on top of the device.
- Safely transport your device in a weather resistant manner.

Security

The District strives to help students make informed choices and exercise accountability when using digital content. In the unlikely situation that a student accesses inappropriate or harmful material, the student is to discontinue use and report the incident to the supervising staff member. Any student identified as a security risk or as having violated the Responsible Use Guidelines may be denied access to the District's system. Other consequences may also be assigned. A student who knowingly brings 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 Board-approved Student Code of Conduct.

Content/Third-Party Supplied Information

Students and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communication systems, such as chat rooms and social media, in the global electronic network that may contain inaccurate and/or objectionable material. It is the student's responsibility to make ethical decisions when interacting in an online environment.

Commercial and Political Use

Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited. Marketing by Non-NISD Organizations Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited. Users may not use their accounts for non-school related activities including but not limited to: financial gain, personal advertising, promotion, non-government related fundraising, or public relations, political advertising, or religious proselytizing.

Email

All students will be issued email accounts. As appropriate, students will use these email accounts for educational purposes. This includes sharing work and communicating digitally with classmates, teachers and parents. Students should keep personal and confidential information private. This means they should not share address, phone number, or any other personally identifiable information about themselves or others. If you should receive an inappropriate or questionable email, you are encouraged to immediately notify an adult and send an email to abuse@nisdtx.org. The district uses multiple email security systems to scan both inbound and outbound email for spam, viruses, appropriate content, attachments, and bulk marketing. This means the system blocks access to language and visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors. Parents wishing to deny access to District email must request this in writing to the campus principal.

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, with respect to any services provided by the system and any information or software contained therein. The District does not guarantee 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. The District makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Acknowledgment and Agreement

I have read and will abide by these Responsible Use Guidelines and understand use of technology resources is a privilege, not a right. I understand that if I fail to comply with these Guidelines, I will be subject to appropriate disciplinary consequences. My signature on the Acknowledgment in Student and Parent Guidebook and Student Code of Conduct as appropriate, confirms my receipt of these Guidelines and my agreement to follow them as a condition of access to District Technology Resources.