



Nederland Independent School District

Student Teacher Acceptable Use Policy

Nederland Independent School District (NISD) provides student teachers with access to district technology resources, including devices, electronic communications systems, networks, accounts, and district-approved digital tools, solely for purposes related to instructional duties performed under the supervision of a cooperating teacher. Access to these resources is a privilege, not a right, and with this access comes the responsibility to use district technology resources in a lawful, ethical, and professional manner.

Student teachers should not expect privacy in content, files, communications, or activity created, stored, accessed, or transmitted using district devices, accounts, networks, or district-approved digital tools. The District may monitor, access, review, audit, or disclose such activity to maintain system integrity, ensure responsible use, comply with legal and safety requirements, and enforce district policy.

Consequences for inappropriate use may include immediate suspension or revocation of access to district technology resources, removal from placement, notification to the partnering university or preparation program, financial liability for damages or remediation costs, and or disciplinary or legal action in accordance with applicable laws and district policy.

District technology resources provide access to a content filtered environment in accordance with applicable law and district policy. While the District uses reasonable filtering and security measures to restrict access to inappropriate material, it is not possible to prevent all access. Student teachers are responsible for following all guidelines for appropriate and responsible use.

NISD is not liable for inappropriate use of technology resources, violations of copyright or other laws, user error or negligence, or costs incurred through misuse of district systems. Availability of technology resources is not guaranteed, and the District is not responsible for the loss of data stored on district devices, servers, or cloud based systems. No representations are made regarding the accuracy, appropriateness, quality, or usability of information accessed through district technology resources. The District will cooperate fully with local, state, or federal officials in any investigation related to misuse of district technology resources.

In addition to the core Acceptable Use Policy requirements, student teachers are subject to the following limitations regarding access to district technology resources:

- Student teachers may use technology resources solely for instructional purposes under the supervision of a cooperating teacher.
- Student teachers may not access confidential student information systems or records unless expressly authorized by district administration and in accordance with district policy.
- Student teachers may not communicate with students using personal electronic devices, personal email accounts, or personal social media platforms.

All student teachers of Nederland ISD must adhere to the following standards of responsible use:

1. District technology resources must be used solely for purposes directly related to assigned instructional duties.
2. Student teachers should not expect privacy in files, communications, activity, or content created, stored, accessed, or transmitted using district devices, accounts, networks, or district approved digital tools.
3. Student teachers are responsible at all times for their use of district technology resources and are expected to act ethically, professionally, and responsibly.
4. Student teachers must comply with all applicable federal, state, and local laws, as well as district policies and procedures.
5. Student teachers must not access, modify, copy, download, or distribute district systems, files, or data except as required to perform assigned instructional duties.
6. The waste or abuse of district technology resources, including excessive bandwidth use or activities that degrade system performance, is prohibited.
7. Altering, damaging, or attempting to modify district computers, networks, printers, security systems, or other district technology is prohibited.
8. Tampering with, removing, relocating, or connecting unauthorized equipment to district technology resources without written authorization is prohibited.
9. Student teachers must protect the confidentiality of all district, staff, and student information, including data protected under FERPA, the Texas Public Information Act, and other applicable laws.
10. Student teachers must safeguard account credentials and must not share usernames, passwords, access tokens, or authentication information or allow others to use their assigned accounts.
11. Student teachers may not permit students or unauthorized individuals to access district systems, devices, applications, or data using student teacher credentials or authenticated sessions.
12. Student teachers must not disable, bypass, attempt to bypass, or interfere with district security systems, monitoring tools, or content filtering controls.
13. Student teachers may not attempt to test, probe, scan, or assess the security of district systems. Suspected vulnerabilities must be reported immediately to district administration.
14. Attempting to destroy, disrupt, disable, or gain unauthorized access to district equipment, district data, the data of other users, or external systems connected to district networks is prohibited.

15. Uploading, creating, transmitting, or executing malicious software, harmful code, scripts, or executables is prohibited.
16. Encrypting, concealing, or deliberately obscuring communications, files, or activity for the purpose of avoiding district monitoring or security review is prohibited.
17. District data may not be stored on personally owned devices or non district systems unless explicitly authorized by the District and secured with appropriate safeguards.
18. Entering district, staff, or student data, including personally identifiable information, into non approved applications, cloud services, or artificial intelligence tools is strictly prohibited.
19. Artificial intelligence tools may be used only for district approved instructional purposes and under the supervision of the cooperating teacher.
20. Student teachers must comply with all applicable copyright, intellectual property, and licensing laws. This includes not copying, streaming, distributing, or using copyrighted or AI generated content without proper authorization.
21. Streaming or displaying copyrighted content from personal accounts for group or public viewing using district technology resources is prohibited.
22. Creating, accessing, transmitting, or displaying content that is abusive, obscene, sexually explicit, threatening, harassing, discriminatory, or illegal is prohibited.
23. Recording, photographing, or distributing audio, video, or images of students, staff, or district facilities without prior administrative authorization is prohibited.
24. Accessing or posting to personal social media platforms using district technology resources for non district purposes is prohibited.
25. If inappropriate content or security concerns are encountered, student teachers must immediately discontinue access and report the incident to district administration.
26. Use of district technology resources for personal financial gain, commercial purposes, political lobbying, or non district business is prohibited.



Nederland Independent School District
Student Teacher Acceptable Use Policy

I have read and understand the Nederland Independent School District Student Teacher Acceptable Use Policy for Technology Resources and agree to comply with the requirements and expectations outlined in this policy.

I understand that access to NISD technology resources is a privilege and that inappropriate use may result in suspension or revocation of access, removal from placement, financial liability, and or legal action in accordance with district policy and applicable law.

In consideration for the privilege of using NISD technology resources, I consent to the monitoring and review of my activity, communications, and use of district devices, accounts, networks, and digital tools for security, compliance, and system integrity purposes.

I release NISD, its employees, agents, and affiliated entities from any and all claims or damages arising from my use of, or inability to use, NISD technology resources.

Name (Printed): _____

Signature: _____ Date: _____

This agreement must be signed prior to being granted access to district technology resources and may be required to be renewed annually or upon contract renewal.