



Nederland Independent School District

Employee Acceptable Use Policy

Nederland Independent School District (NISD) provides employees with access to district technology resources, including devices, electronic communications systems, networks, accounts, and district-approved digital tools, solely for purposes related to the performance of assigned job duties and district responsibilities. 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.

Employees 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, disciplinary or administrative action up to and including termination of employment, financial liability for damages or remediation costs, and/or legal action in accordance with applicable laws and district policy.

District technology resources provide access to systems and information necessary to perform district business. While the District employs reasonable security and monitoring measures, it is not possible to prevent all misuse or unauthorized activity. Employees are responsible for following all guidelines for appropriate and responsible use.

NISD is not liable for an employee's 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.

Employees must return all district-owned equipment, devices, records, and technology resources in their possession upon request by the District or upon separation from employment. If an employee is in possession of records, whether written or electronic, that are subject to district records retention requirements and are believed to be the sole copy, the employee must

return those records to the District. Employees must not retain copies of district records containing confidential or sensitive information. Any remaining confidential or sensitive records in the employee's possession must be securely deleted, destroyed, or shredded in accordance with district procedures and applicable law.

All employees 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 job duties and district responsibilities.
2. Employees are responsible at all times for their use of district technology resources and are expected to act ethically, professionally, and responsibly.
3. Employees must comply with all applicable federal, state, and local laws, as well as district policies and procedures, including the Family Educational Rights and Privacy Act (FERPA), the Texas Public Information Act, records retention requirements, and confidentiality statutes.
4. Employees must not access, modify, copy, download, or distribute district systems, files, or data except as required to perform assigned job duties.
5. The waste or abuse of district technology resources, including excessive bandwidth use or activities that degrade system performance, is prohibited.
6. Altering, damaging, or attempting to modify district computers, networks, printers, security systems, or other district technology is prohibited.
7. Tampering with, removing, relocating, or connecting unauthorized equipment to district technology resources without written authorization is prohibited.
8. Employees 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. Employees must use appropriate professional judgment, language, and tone in all electronic communications. Communications sent using district systems or accounts may reasonably be perceived as representing the District and must reflect professionalism and accuracy.
9. Employees must safeguard account credentials and must not share usernames, passwords, access tokens, or authentication information, including substitutes, or allow others to use their assigned accounts.
10. Employees may not permit students or unauthorized individuals to access district systems, devices, applications, or data using employee credentials or authenticated sessions.
11. Employees must not disable, bypass, attempt to bypass, or interfere with district security systems, monitoring tools, or content filtering controls.
12. Employees may not attempt to test, probe, scan, or assess the security of district systems. Suspected vulnerabilities must be reported immediately to district administration.
13. 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.
14. Uploading, creating, transmitting, or executing malicious software, harmful code, scripts, or executables is prohibited.
15. Encrypting, concealing, or deliberately obscuring communications, files, or activity for the purpose of avoiding district monitoring or security review is prohibited.

16. 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.
17. Entering district, staff, or student data, including personally identifiable information (PII), into non-approved applications, cloud services, or artificial intelligence (AI) tools is prohibited.
18. Artificial intelligence (AI) tools may be used only for district-approved purposes and in accordance with professional expectations, confidentiality requirements, and instructional integrity.
19. Employees 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.
20. Streaming or displaying copyrighted content from personal accounts for group or public viewing using district technology resources is prohibited.
21. Creating, accessing, transmitting, or displaying content that is abusive, obscene, sexually explicit, threatening, harassing, discriminatory, or illegal is prohibited.
22. Recording, photographing, or distributing audio, video, or images of students, staff, or district facilities without prior administrative authorization is prohibited.
23. Accessing or posting to personal social media platforms using district technology resources for non-district purposes is prohibited. Employees are held to professional standards in their use of social media when representing, or when reasonably perceived as representing, the District.
24. Employees may not communicate electronically with students using district technology resources unless authorized and in accordance with district policy, professional standards, and any limitations established by the Superintendent or designee.
25. If inappropriate content or security concerns are encountered, employees 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.
27. Use of district email distribution lists or mass communication tools is restricted to official district business. Distribution lists may be used only by administrators or employees expressly authorized by the Superintendent or designee and may not be used for personal, commercial, political, or non-district purposes.



Nederland Independent School District

Employee Acceptable Use Policy

I have read and understand the Nederland Independent School District Employee 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, disciplinary action up to and including termination of employment, 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.

Employee Name (Printed): _____

Signature: _____ Date: _____

This agreement must be acknowledged prior to being granted access to district technology resources and may be required to be renewed periodically or upon policy revision.