



Nederland Independent School District

Trustee Acceptable Use Policy

Nederland Independent School District (NISD) provides Trustees with access to district technology resources, including devices, electronic communications systems, networks, accounts, and district-approved digital tools, for purposes related to governance responsibilities and official district business. 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.

Trustees 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 requirements, and enforce district policy.

Consequences for inappropriate use may include suspension or revocation of access to district technology resources, referral for board action, 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 information necessary for governance and oversight. While the District employs reasonable security and monitoring measures, it is not possible to prevent all misuse or unauthorized activity. Trustees 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, trustees:

- Are provided access primarily for governance and district business purposes.
- Must ensure electronic communications reflect professional standards and board responsibilities.

- Trustees may access confidential district information only as necessary to fulfill governance responsibilities and must maintain strict confidentiality in accordance with applicable law.
- Trustees may not use district technology resources to conduct deliberations or communications that would violate the Texas Open Meetings Act or other applicable laws.
- Trustees may not use personal email accounts, personal devices, or personal communication platforms to conduct official district business in a manner that circumvents district record retention, public information, or transparency requirements.

All trustees 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 governance responsibilities and official district business.
2. Trustees 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. Trustees are responsible at all times for their use of district technology resources and are expected to act ethically, professionally, and in accordance with board governance standards.
4. Trustees must comply with all applicable federal, state, and local laws, including the Texas Open Meetings Act, the Texas Public Information Act, records retention requirements, and confidentiality statutes.
5. Trustees must not access, modify, copy, download, or distribute district systems, files, or data except as necessary to fulfill governance responsibilities.
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. Trustees must protect the confidentiality of all district, staff, and student information, including data protected under FERPA and other applicable laws.
10. Trustees must safeguard account credentials and must not share usernames, passwords, access tokens, or authentication information or allow others to use their assigned accounts.
11. Trustees must not permit unauthorized individuals to access district systems, devices, applications, or data using trustee credentials or authenticated sessions.
12. Trustees must not disable, bypass, attempt to bypass, or interfere with district security systems, monitoring tools, or content filtering controls.
13. Trustees 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 legal compliance requirements 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 purposes and must not compromise confidentiality, governance responsibilities, or legal compliance.
20. Trustees must comply with all applicable copyright, intellectual property, and licensing laws.
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 proper authorization is prohibited.
23. Use of district technology resources for personal financial gain, commercial purposes, political campaigning, or non district business is prohibited.
24. Trustees must ensure that all electronic communications related to district business are retained, archived, and accessible in accordance with records retention and public information requirements.
25. If inappropriate content or security concerns are encountered, trustees must immediately discontinue access and report the incident to district administration.



Nederland Independent School District

Trustee Acceptable Use Policy

I have read and understand the Nederland Independent School District Trustee 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 revocation of access, board action, 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 acknowledged prior to being granted access to district technology resources and may be required to be renewed periodically or upon policy revision.