

Port Neches-Groves Independent School District

Employee Technology Acceptable Use Policy

Port Neches-Groves Independent School District (“PNGISD” or “District”) offers technological opportunities to promote educational excellence in the schools by facilitating safe and effective resource sharing, innovation, and communication through the Internet and other electronic information systems. These Technology Acceptable Use Guidelines are intended to educate users and to set standards which will serve to protect the District. All system users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the District’s technology resources and shall agree in writing to comply with such regulations and guidelines. All such agreements will be maintained for the school year by the administration. Users should read the applicable District and technology policies, administrative regulations, and this agreement form. [See policies CQ and DH, and provisions on use of electronic media in the applicable handbook]

The Port Neches-Groves ISD network has been established for a limited educational purpose. The use of accounts must be in support of educational and/or research and consistent with the educational objectives of PNGISD. The following rules are representative (but not inclusive) of how the PNGISD network, including the Internet, is to be used by employees and other designated individuals. Inappropriate use may result in cancellation of the privilege. Certain state, local, and federal statutes may apply to the electronic communications system and inappropriate uses may also be unlawful. Unlawful use of district electronic resources will be referred to proper authorities. District authorities may also initiate other disciplinary actions.

District Technology and Resources

The following guidelines apply to all District networks, e-mail accounts, devices connected to the District’s networks, and all District-owned devices used on or off school property. Port Neches-Groves ISD electronic communications and data management system includes but is not limited to:

- Computer equipment owned by PNGISD (network or stand-alone)
- Telephones, cell phones, and associated voice mail
- Peripherals include, but are not limited to copiers, external storage devices, video cameras, interactive devices, keyboards, monitors, mice, printers, scanners, web cameras, and digital cameras.
- Servers and network hardware comprising the PNGISD network
- Software installed (with Technology Department authorization) and/or subscriptions licensed to PNGISD on any networked or stand-alone device.
- Digitized information including faxes, stored text, data files, email, digital images, video files, and audio files
- District-provided filtered Internet access (wired and wireless)
- E-mail accounts including access to cloud-based (online) document storage and collaboration space (e.g., Microsoft Office 365 and Google Workspace for Education)
- New technologies as they become available

Disclaimer

As required by the Children’s Internet Protection Act (CIPA), the district maintains a filtering system that blocks access to information considered obscene, pornographic, and inappropriate for students or harmful to minors as defined by the federal CIPA guidelines. The Internet is a network of many types of communication and information networks. It is possible to access material that you might find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to always prevent such access. It will be the user’s responsibility to follow the rules for appropriate use. PNGISD makes no warranties for the access it provides. The District shall not be liable for inappropriate use of the District’s technology resources, violations of copyright restrictions or other laws, mistakes, negligence, or costs incurred by a user. The District shall not be responsible for ensuring

Port Neches-Groves Independent School District

Employee Technology Acceptable Use Policy

the availability of the District's technology resources or the accuracy, age appropriateness, or usability of any information found on the Internet.

Privilege

Access to resources is a privilege, not a right. Electronic mail and use of other PNGISD resources is not confidential and may be monitored at any time by designated District staff to ensure appropriate use for educational or administrative purposes. This monitoring may include activity logging, virus scanning, and content scanning. All district email and electronic communication is subject to open records.

Rules for Responsible Network and Computer Use

- Users are assigned an individual account for access to approved District technology resources and are responsible for keeping account information private. Do not share password credentials with other users.
- The district's technology resources are primarily for administrative and instructional purposes. Limited personal use is permitted if the use imposes no tangible cost to the district, does not unduly burden the district's technology resources and has no adverse effect on job performance or on a student's academic performance.
- All software must be reviewed for network and hardware compatibility by the Technology Department prior to authorization of purchase, donation, or use.
- Users must comply with the Public Information Act, the Family Educational Rights and Privacy Act (FERPA), and any other applicable law or policy regarding records retention and confidentiality of student and District records.
- Do not load or place any software, viruses, or games on any district computer or system connected to the district's system.
- Users shall not bypass PNGISD security measures and Internet filter through means such as, but not limited to, online proxies, bootable media, IP spoofing, etc.
- No one should attempt to write, produce, generate, copy, propagate or introduce any computer code designed to self-replicate, damage, change, or otherwise hinder the performance of any computer's memory, file system, or software.
- It is prohibited to knowingly or recklessly post false or defamatory information about a person or an organization.
- Do not attempt to harm equipment, materials, or data
- Users must not post any information that could cause damage in any way or cause any danger or disruption to the District.
- The user is always responsible for proper use of his/her account.
- The district wireless network is used to provide filtered Internet access and may have limited access to other district network resources.
- Employees must maintain the confidentiality of health or personnel information concerning colleagues and students unless disclosure serves lawful professional purposes or is required by law.
- Copies of potentially sensitive or confidential District records should not be sent, viewed, or stored using an online application that has not been approved by the District.
- Email public distribution lists should only be used by administrators and/or their designee. Email lists should only be used for school business.
- When communicating through e-mail or other electronic means, users must use appropriate language and etiquette. Individuals who receive e-mail from a district address may believe the message represents the District's point of view.

Port Neches-Groves Independent School District

Employee Technology Acceptable Use Policy

- The e-mail system should not be used to disseminate material or information on the behalf of or about professional unions, collective bargaining, private businesses or associations, or political campaigns or organizations without express written consent of the Superintendent or his/her designee.
- Only authorized District staff may communicate with District students through electronic means, including social media, e-mail, and text messaging. If you are unsure whether you are authorized to communicate with a student through electronic means, ask an immediate supervisor. [See Employee Handbook and Local Policy DH]
- Users must immediately report any suspicious behavior or other misuse of technology to supervisor or campus administrator.

Use of Personal Electronic Devices

- Employees should not maintain district information on privately owned devices. Any district information must be forwarded or transferred to the district to be preserved.
- Personal electronic devices can only be connected wirelessly to the district network. Personal electronic devices will be filtered in the same manner as District owned devices on the PNGISD wired network. Connecting any personal devices to district wired network resources is prohibited.
- It is the responsibility of the owner to ensure that all software and files on personal devices are licensed for use in compliance with copyright law
- Personal electronic devices are to have the most recent operating system and security software, including but not limited to antivirus software, installed, and maintained.
- All peer-to-peer (music/video/file-sharing) software or web-hosting services on personal electronic devices must be disabled while connected to the district wireless network.
- Users are responsible for appropriate use of any electronic communication device.
- The PNGISD network will be filtered to meet Child Internet Protection Act requirements. (*Port Neches- Groves ISD will not be responsible for monitoring inappropriate sites visited while connected to a personal service provider*).
- PNGISD reserves the right to revoke any or all network privileges due to misuse of the Port Neches-Groves ISD wireless network.
- Port Neches-Groves ISD will not be responsible for providing technical support on personal electronic devices.
- Users may not use their personal device inside or outside of the classroom in a way that disrupts the educational environment, violates the rights of others, or invades the privacy of others. This includes, but is not limited to, using the device to cheat, to violate the Student Code of Conduct rules, to harass or bully students or staff, and/or for unlawful purposes.
- PNGISD is not responsible for damage, loss or theft of any personal electronic device, software, or services. The District assumes no liability for any loss or damage to any personal devices.
- PNGISD will not be responsible for financial obligations arising from the unauthorized use of networks.
- PNGISD is not responsible for the accuracy or quality of the information obtained or stored on the network or retrieved via the internet.

Inappropriate Use

The following uses of the Port Neches-Groves ISD Network are considered unacceptable:

- Using the resources for any illegal purpose, including threatening school safety.

Port Neches-Groves Independent School District

Employee Technology Acceptable Use Policy

- Accessing the resources to knowingly alter, damage, or delete District property or information, or to breach any other electronic equipment, network, or electronic communications system in violation of the law or District policy.
- Damaging electronic communication systems or electronic equipment, including knowingly or intentionally introducing a virus to a device or network, or not taking proper security steps to prevent a device or network from becoming vulnerable.
- Disabling or attempting to disable or bypass any Internet filtering device.
- Encrypting communications to avoid security review.
- Using another person's account without permission.
- Pretending to be someone else when posting, transmitting, or receiving messages.
- Attempting to read, delete, copy, modify, or interfere with another user's posting, transmittal, or receipt of electronic media.
- Using resources to engage in conduct that harasses others.
- Sending, posting, or possessing materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including material that constitutes prohibited harassment and "sexting."
- Using inappropriate language such as cursing, vulgarity, ethnic or racial slurs, and any other inflammatory language.
- Violating others' intellectual property rights, including downloading or using copyrighted information without permission from the copyright holder.
- Posting or transmitting pictures of students without obtaining prior permission from all individuals depicted or from parents of depicted students who are under the age of eighteen.
- Wasting school resources through improper use of the District's technology resources, including sending spam.
- Gaining unauthorized access to restricted information or resources.
- Transmission of any material in violation of any US or state regulation is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material, or material protected by trade secret.

Artificial Intelligence

The purpose of this policy is to ensure that the use of Artificial Intelligence (AI) platforms at PNGISD are conducted in a lawful, ethical, and responsible manner. This policy aims to:

- Promote compliance with copyright and infringement laws to prevent unauthorized use of copyrighted materials.
- Safeguard the privacy and security of individuals by prohibiting the processing of Personally Identifiable Information (PII).
- Encourage adherence to data protection regulations and industry best practices.
- Establish guidelines for ethical usage of AI services to prevent harm and promote positive contributions.

Rules for Acceptable Artificial Intelligence Use

- Only use copyrighted materials with proper authorization, such as licensing or fair use exceptions.
- Do not use AI platforms to generate content that infringes upon the intellectual property rights of others.

Port Neches-Groves Independent School District

Employee Technology Acceptable Use Policy

- Respect the terms of use and licenses associated with datasets, models, and content used in AI processes.
- Adhere to all applicable local, national, and international laws, regulations, and industry standards.
- Seek legal advice if uncertain about the legality of using AI platforms for specific purposes.
- Comply with data protection regulations, including obtaining proper consent and managing data securely.
- AI platforms must not be used to process, store, or transmit any Personally Identifiable Information (PII) without proper consent and compliance with applicable data protection regulations (e.g., GDPR, HIPAA, COPPA, FERPA).
- PII includes but is not limited to names, addresses, phone numbers, email addresses, social security numbers, and financial information.
- Anonymization or pseudonymization of data is not sufficient when it comes to protecting sensitive information.
- Use AI platforms to promote positive outcomes and avoid generating harmful, offensive, or discriminatory content.
- Refrain from using AI platforms for malicious activities, misinformation, or any actions that could negatively impact individuals or groups.

Prohibited Artificial Intelligence Use

- Do not engage in any form of illegal, fraudulent, or unauthorized activities using AI services.
- Avoid using AI platforms to create content that is defamatory, harassing, abusive, threatening, or obscene.
- Do not distribute malware, viruses, or engage in any actions that compromise the security or integrity of systems.

CONSEQUENCES FOR INAPPROPRIATE USE

Noncompliance or inappropriate use may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Violation of law may result in criminal prosecution as well as disciplinary action by the District.

REPORTING VIOLATIONS

Users should immediately report any known violation of the District's applicable policies, District policy, or acceptable use guidelines to the Technology Director, immediate supervisor, or campus administrator. Users should immediately report requests for personally identifiable information, as well as any content or communication that is abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal to the Technology Director, immediate supervisor, or campus administrator.

RETURN OF TECHNOLOGY RESOURCES AND RECORDS

Upon leaving employment, employees must return any equipment or records, written or electronic, to the District for records retention if it is believed they are retaining the sole copy of a record subject to records retention requirements.