

# **Prosper ISD**

## **Staff Responsible Use Policy**



## Overview

It is the policy of Prosper ISD (PISD) to maintain an environment that promotes ethical and responsible conduct with all electronic resources and activities. Use of district resources is a privilege and carries associated user responsibilities.

When signing the PISD Responsible Use Policy, you, as a PISD employee, partner, or other permitted user of PISD electronic resources and equipment (“user”), acknowledge that you understand, accept, and agree to abide by the information and requirements outlined in this document.

Users understand and agree that:

1. The Technology Department has the authority to enforce this policy, including disabling accounts, restricting access, or confiscating equipment when necessary to protect District systems or data.
2. Users acknowledge that PISD may remotely disable, lock, or wipe District-owned devices or accounts if equipment is lost, stolen, compromised, or upon separation from the District.
3. The use of PISD equipment (“PISD Equipment”) and associated technology is a privilege, not a right.
4. The terms “PISD Equipment,” “equipment,” and “device”, including equipment purchased with grant funds, booster clubs funds, etc., refer to any device or associated accessories such as computers, printers, tablets, batteries, power cords/chargers, cases, keyboards, mice, scanners, document cameras, docking stations, charging carts, etc. All equipment and digital resources are the property of PISD.
5. The terms “software” or “services” refer to any applications or tools, internal or online, provided by PISD, including software purchased with grant funds, booster club funds, etc. Software or services licensed by the District are the property of PISD.
6. There is no expectation of privacy for Users when using PISD technology resources. All data and files stored on and network activity involving PISD Equipment, the District’s network, and/or the cloud are subject to review and monitoring.
7. PISD retains ownership and control of any and all of its hardware, software, equipment, data, documents, or supplies placed in an Alternative Work Site, including telework, in connection with an authorized arrangement under this policy. Only portable PISD Equipment, such as laptops, and similar equipment and related accessories, may be transferred to an Alternative

Work Site, and all such items must be promptly returned to PISD's possession, custody, and control upon termination of an authorized telework arrangement, or upon request by PISD at any time.

8. If any other PISD Equipment is needed at an Alternative Work Site, users must submit a Technology Helpdesk ticket.
9. Users are encouraged to take their assigned laptops home each day. However, Users are not permitted to take other designated work or placement location devices (such as document cameras, monitors, printers, scanners, etc., used in the performance of job or placement responsibilities) home without prior written authorization from the Technology Department. If a User is given permission to take a District device home, the user is held to the same District Responsible Use Policy.
10. All intellectual property—including digital products, inventions, and creative works—developed by Users during employment or using District resources is considered a "work made for hire", specifically ordered or commissioned for use by the District as a collective work or as part of an audiovisual work, translation, supplementary work, compilation, or instructional text, and remains the exclusive property of the District. Users may not alter, destroy, or disclose any such property or sensitive data, including student personally identifiable information (PII), without authorization. This provision shall survive after the User's termination of employment with the District.
11. If a tool, web app, app, artificial intelligence (AI), or other software program is not on the approved software list, staff members must submit a request through LearnPlatform for approval consideration. Only software listed in the approved software list is permitted for use.
12. Users are prohibited from using personal or their primary district accounts to create or administer any digital service that represents the District or any PISD school, program, or club. This includes, but is not limited to, social media accounts, websites, and YouTube channels. All such digital representations must be approved by District Administration, with access configured in coordination with PISD Technology to ensure compliance with District standards and security protocols.
13. Students should never be given credentials to any District resource or account managing the District's digital representation without the approval of District Administration and PISD Technology to ensure compliance with District standards and security protocols.

14. Users must comply with the PISD Responsible Use Policy at all times when using devices or digital resources provided by PISD. Users must also comply with the PISD Responsible Use Policy when using their PISD devices on school property, at school-related events, and while performing PISD duties outside of District facilities, such as at training, conferences, and telework settings.
15. Users must follow PISD security precautions, such as keeping their username and password confidential at all times. Users may log in only with their District-assigned username. Users must not share their passwords, pictographs, or employee ID numbers with other Users.
16. Users should not use their PISD username or email address when signing up for services unrelated to official PISD business.
17. By following best cybersecurity practices, users should not use their PISD password or any variations of it when signing up for any services. This includes services that may be used for official PISD business and those approved by Teaching and Learning.
18. If a User believes that his/her username, password, or two-factor authentication device (phone, hardware key, USB security key) has been compromised in any way, the User must contact the Technology Department immediately to assess the situation.
19. Users remotely accessing PISD network resources or PISD internet services, such as Gmail, from a public network must use a PISD device with standard security configurations and utilize the District's official Virtual Private Network (VPN) client to ensure proper security.
20. The access key cards (Badges) are assigned to you individually and may not be shared or handed out to anyone at any time. Sharing any personally assigned PISD Equipment, including Badges, compromises PISD's security and violates District policy.
21. Users agree to adhere to the standards set forth annually in the Confidentiality Agreement and by law, including FERPA, by treating any PISD information, including, but not limited to, student education records, staff personnel records, student or staff medical records, personally identifiable information, network or computer security information, and student or staff network or computer activity information as confidential. Specifically, Users should never share or otherwise disclose sensitive information, securely or otherwise, to a broader audience than is approved or to anyone who does not have a legitimate educational interest as defined by FERPA.
22. Users shall also comply with Board Policy FL, including all requirements related to access and disclosure. Per Board Policy FL, school officials may access student records only for a legitimate educational interest.

23. Users must not transmit or publish PII, such as social security numbers or passwords, via unsecured methods, such as email or text. Encrypted email or other secured means of document transfer should be used instead.
24. Users should never store PII, educational records, or sensitive data in unapproved areas. All such data must remain accessible only on officially designated systems or in-network storage locations, including PISD-provided Google Workspace for Education and/or District Server Shared Drives. Users shall not store such data or other district-related information on any external media or other external cloud storage.
25. Users will refrain from using, uploading, or sharing employee and student (PII) when using AI tools, even if the tool is in the approved software list.
26. No personally owned, donated, trial, or externally sourced hardware may be connected to or used with PISD systems or networks without prior evaluation and written approval by the Technology Department through the approved LFLaserfiche request process.
27. PISD Equipment shall only be used for PISD job-related purposes. All rules and guidelines for District-provided devices, services, and accounts apply at all times, whether on or off the designated work location.
28. All Users must adhere to all policies of the school, District, and PISD Board, as well as local, state, and federal laws, regulations, and guidelines, whenever applicable.
29. Users are required to keep equipment in good, working condition without alterations, markings, or damage of any kind. Users must remove any stickers, labels, etc., prior to returning equipment at the end of its life.
30. Users are expected to report any damage to their device or associated accessories to a supervisor or campus technician immediately.
31. Users who identify or become aware of a security problem related to District technology are expected to report the details to their supervisors or the Technology Department immediately, without discussing the problem with other employees.
32. If Users discover information, images, messages, or behaviors that are inappropriate, dangerous, threatening, or make them feel uncomfortable, they should immediately report what they observed to a supervisor.
33. Users are prohibited from using PISD resources at school, home, or any location to harass other Users or anyone else.

34. Users are prohibited from accessing, receiving, generating, or distributing any pornographic content and sexually explicit images, websites, content, or materials-
35. Users shall use electronic communication tools (email, messaging, videoconferencing) appropriately to ensure student and staff safety and security
36. Users may not use any PISD or personal resources to maliciously hack, introduce viruses or other malware, or manipulate or modify the files of other Users without permission.
37. All Users are expected to follow existing copyright law (*Title 17, USC*) and educational fair use policies.
38. Requests for technology-related accommodations required under applicable disability laws must be coordinated through Human Resources and the Technology Department.

## **Bring Your Own Device (BYOD)**

BYOD technology is defined as technology used at school that is not owned by PISD.

**Upon hire, the district will assign PISD Equipment to the new employee. While at work or placement at PISD, staff are required to use only the assigned PISD Equipment. Should additional resources be needed to perform your job duties, please contact the Technology Department.**

**The following guidelines must be followed by staff using a personally owned electronic device at work or while on PISD property.**

1. The Technology Department and Campus Administrators have the right to prohibit staff from using video, photographic, or audio recordings on their personal devices, or to restrict the use of any app or feature, as deemed necessary, for privacy, safety, and instructional purposes.
2. The Technology Department and Campus Administrators may prohibit staff from using PISD hardware or connecting to the PISD network with any personal devices or other gaming-related technology software or hardware, such as PlayStations.
3. Staff may not interfere with or circumvent the PISD-Wireless network by using personal devices or software, such as Wi-Fi hotspots, access points, or routers, which could disrupt PISD equipment and/or services due to the introduction of malware or the use of malicious websites.
4. Use of ISD-Wireless through personal phones/smartwatches is primarily intended for instructional use. PISD-Wireless may be shut down entirely to safeguard the network's integrity,

protect Users from malware or malicious actors, or ensure the proper functioning of PISD-owned devices and services.

5. Users are responsible for their own personal phones/smartwatches. PISD will not be responsible for the replacement or repair of any personal device that is damaged or stolen while on District property. Any data and/or SMS/MMS (texting) charges will not be reimbursed by PISD.

## **STATE OF TEXAS SENATE BILL 944**

Senate Bill 944 amends the Texas Public Information Act to address how public information on privately owned devices is preserved and disclosed, subject to applicable public information requests. The law became effective on September 1, 2019. Any public information contained on an employee's personal device, including, but not limited to, any public record stored in text, pictures, or voice recordings, is subject to the Public Information Act.

## **Content Filtering**

While the District uses filtering technologies and protection measures to make a concerted effort to restrict access to inappropriate material, it is not possible to absolutely prevent such access. User compliance with the rules for responsible use as outlined in this agreement increases the effectiveness of the District's protection measures. As access to the PISD network is a privilege, administrators may review files and messages to maintain system integrity and ensure that Users are acting responsibly. When PISD devices are used at other locations, Users must monitor the content accessed on the device.

## **Stolen Equipment**

If District-owned equipment is stolen, a User must contact a supervisor immediately and no later than 48 hours, who will initiate a PISD police report. Failure to report a theft to the administration may result in the loss of the use of a District-provided device.

## **Examples of Misconduct under this Responsible Use Policy**

*Irresponsible conduct includes, but is not limited to, the following, which may result in disciplinary actions:*

- Revealing the personally identifiable information of staff or students
- Falsifying identification documents

- Taking pictures or videos of a student, employee, or community member without his or her permission, regardless of whether these images are intended to be posted online, in a social media app, or otherwise distributed
- Impersonating another employee or student by using their account, password, or pictographs
- Providing a student or another employee access to your account, password, or pictographs
- Obtaining data or passwords belonging to others on the District's network
- Participating or helping others in malicious activity, vandalizing, deletion, or tampering with files, software, equipment, or other components of the District's network
- Posting anonymous messages or unlawful information on the District's network
- Using the District's network for illegal activities, including copyright violations, illegally downloading music, games, images, videos, or other media
- Placing a computer virus or other malware on PISD equipment or the District's network
- Attempting to access blocked sites, bypassing the internet filter, or concealing internet activity
- Engaging in unauthorized downloading or installation of any software
- Using District devices and services for financial or commercial gain, advertising, political action, activities, or lobbying
- Participating in any cyberbullying and/or harassment
- Using inappropriate language, sexting, sending or accessing pornographic content, sending or accessing sexually explicit images, websites, content, or materials, or receiving such materials

## **Consequences of Misuse**

Users are required to abide by the provisions of the District's Responsible Use Policy and administrative procedures. Failure to do so can result in suspension of access or termination of privileges and may lead to disciplinary procedures, legal actions, or termination of employment (where applicable). Users with questions about computer use and data management can contact the Chief Technology Officer.