

Prosper ISD

Student Responsible Use Policy



Overview

We believe technology is a tool that enables our students to learn the curriculum more deeply, and that the curriculum is the driving force behind technology use in the classroom.

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 for parents and students.

When signing the PISD Student Responsible Use Policy, you are acknowledging that you understand, accept, and agree to abide by the information and requirements outlined in this document:

PISD students and parents/guardians understand and agree that:

1. PISD reserves the right to restrict access to technology at any time.
2. The use of PISD equipment and associated technology is a privilege, not a right.
3. The terms "PISD Equipment," "equipment," and "device" refer to any device or associated accessories, such as computers, printers, tablets, student identification badges, 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.
4. The terms "software," "app or application," and "services" refer to any applications or tools, internal or online, provided and licensed that are the property of PISD.
5. 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.
6. Students and families must comply with the PISD Responsible Use Policy at all times when using technology or digital resources provided by PISD, or when using their own devices on District property or at school-related events.
7. All rules and guidelines for District-provided equipment, services, and accounts apply at all times, on or off campus.
8. Students are not permitted to take classroom devices home without prior written authorization from the Technology Department. If a student is given permission to take a District device home, the student's parent or guardian will be asked to sign a Student Device Equipment Checkout form, which documents the device information.
9. All users must comply with the policies of the school, District, and PISD Board, and with local,

state, and federal laws, as applicable.

10. Students are expected to keep equipment in good working order, free of markings or damage. Failure to do so may result in the consequences outlined in the Student Code of Conduct.

11. Students are expected to notify campus Technology or administration immediately if their device or associated accessories are damaged. If equipment is used inappropriately, lost, damaged, or simply neglected, disciplinary consequences may result, along with fees consistent with the damage. Please visit [this link for more information about fees.](#)

12. Students who identify or become aware of a security problem related to District technology shall immediately convey the details to their teacher, counselor, school administrator, Technology personnel, or use the district's Tip 411 system, without discussing the problem with other students.

13. Students are prohibited from accessing faculty, administration, staff, or other students' devices, files, or accounts for any reason without explicit permission from that user. Students shall not use any method to obtain control of another individual's device through any means, including through the use of the Student's own personal devices.

14. If a student believes their username, password, or pictograph has been compromised in any way, they must contact a teacher, an administrator, or Technology immediately.

15. If a student discovers information, images, messages, or behaviors that are inappropriate, dangerous, threatening, or cause discomfort, the student shall immediately notify a teacher, counselor, or school administrator or use the district's Tip 411 system, without discussing it with other students.

16. Students are prohibited from using PISD resources at school, home, or any other location to harass any individual, including, but not limited to, other students or staff.

17. Students may not use any PISD or personal resources at school or at home to maliciously hack, introduce viruses or other malware, or manipulate or modify others' files without permission.

18. Students may not use, upload, disclose, or share employee or student personally identifiable information (PII).

19. Students may not destroy or alter any PISD digital products, resources, educational records, intellectual property, or work products of any kind. Students shall take special care to avoid destroying, altering, exfiltrating, sharing, or otherwise disclosing any such digital products, resources, records, intellectual property, or work product of any kind containing student educational records, PII, or other sensitive information.

20. Students are expected to follow copyright law ([Title 17, USC](#)) and educational [fair use](#) policies.

21. Students may log in only with their District-assigned username. Students must not share their

passwords, pictographs, or student ID numbers with other students.

22. PISD may remove a user's access to the network/cloud storage, email, or any other service without notice at any time if a user is engaged in any unauthorized activity.

23. The student identification 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.

Bring Your Own Device (BYOD)

BYOD is the use of privately owned devices, rather than PISD-owned devices, at school. Students are not permitted to use BYOD technology without express authorization from school administrators. All students using any device, including BYOD devices, at school, on PISD property, or during PISD activities and events are subject to this Responsible Use Policy and all other applicable District and State policies and guidelines. Any device may be removed from a student's possession upon suspicion of violation of these policies or the Student Code of Conduct.

The following guidelines must be followed by students using a BYOD device at school:

1. Campus administrators and teachers have the right to prohibit students from using video, photographic, or audio recording on their personal devices (including phones, smart watches, and GPS parental trackers) or restrict the use of any app or feature as deemed necessary for the purposes of classroom privacy, safety, and instruction.
2. Administrators may examine a student's BYOD device and search its contents if there is reason to believe the Responsible Use Policy has been violated.
3. Devices operated by students at school must utilize the PISD-Wireless network.
4. Students may not interfere with or circumvent the PISD-Wireless network by using personal networking devices or software, such as Wi-Fi hotspots or access points, which could disrupt PISD Equipment or services due to the introduction of malware or the use of malicious websites.
5. Use of the PISD-Wireless via BYOD devices is intended solely for instructional use. PISD-Wireless may be shut down entirely to safeguard the network's integrity, protect students from malware or malicious actors, or ensure the proper functioning of PISD-owned devices and services.
6. Students are responsible for safeguarding their own personal devices. PISD will not be liable for the replacement or repair of any personal device that is damaged or stolen.
7. Students are responsible for their device setup, maintenance, and charging. Employees will not

store a student's device unless the device was taken up as a disciplinary action or for testing. No District employee will diagnose, repair, or work on a student's personal device.

8. Personal and PISD devices have monetary value. Students are prohibited from stealing, trading, or selling these items to/from anyone. If a student finds another individual's personal or PISD device(s), the student must report it to the campus technician or an administrator.
9. Students are prohibited from engaging in e-commerce using PISD Equipment or their own devices while in PISD facilities.

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. Student compliance with the rules for responsible use as outlined herein increases the effectiveness of the District's protection measures. As access to the PISD network is a privilege, administrators and faculty may review files and messages to maintain system integrity and ensure that users are acting responsibly. When PISD devices are used at other locations, the District expects parents and guardians to monitor the content accessed on those devices.

Stolen Equipment

If District-owned or personal equipment is stolen, a student must contact an assistant principal or a principal, who will initiate a PISD police report. Failure to report a theft to school administration may result in the loss of use of a District-provided device for a student and in the payment of the applicable fees, as listed in [this link](#).

Examples of Misconduct under this Responsible Use Policy

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

- Any use of technology resources that are deemed disruptive, including sending mass emails, using devices with disruptive audio settings, or other behavior deemed disruptive by classroom teachers or administrators
- Deleting browser history
- Revealing the personally identifiable information of staff or students

- Falsifying identification documents
- Taking or manipulating, including AI-generated content, pictures, or videos of a student, staff member, or community member without their permission, regardless of whether these images are intended to be posted online, in a social media app, or otherwise distributed
- Posting, reposting, or broadcasting information, including alleged criminal allegations or mugshots, of any student, staff, or community member on any PISD digital resource
- Obtaining or using someone else's account, pictograph, or password, or allowing one's own password and/or pictograph to be used by someone else
- Using the District's network for disruptive or illegal activities, including mass emailing, copyright violation, software license or service contract violations, illegally downloading music, games, images, videos, or other media, or harassment
- Vandalizing and/or tampering with equipment, programs, files, software, or other components of the District's network, including using or possessing malicious software, is prohibited
- Unauthorized alteration, tampering, copying, distributing, taking a picture or screenshot, or other modification of another individual's or team's information or work product, regardless of the media type
- Unauthorized modifications, deletion, or distribution of data stored within District systems
- Gaining unauthorized access anywhere on the District's network
- Participating in malicious activity on the District's network, or helping others to participate in an unauthorized activity on the District's network
- Posting anonymous messages or unlawful information on the District's network
- Placing a computer virus or other malware on PISD Equipment or the District's network
- Attempting to access blocked sites, bypassing the internet filter, use of proxies, or concealing internet activity
- Legally downloading or streaming music, games, images, videos, or other media without the permission of a teacher
- Unauthorized downloading or installation of any software, including shareware and freeware
- Using District devices and services for financial or commercial gain, advertising, political action, activities, or lobbying
- Off-task accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, or helping others to do so
- Engaging third-party sites to provide students with information or links that otherwise would be

considered malicious in nature or could potentially become malicious

- Emailing staff and students in a way that could be considered “spam” or unsolicited email
- Sending or forwarding non-school-related messages, including harassing or disruptive messages, chain letters, advertisements, or other messages that include many recipients
- Participating in any cyberbullying and/or harassment
- Using inappropriate language, sexting, sending or accessing pornographic content, sending or accessing sexually inappropriate images, content, or materials, or receiving such materials without notifying a PISD employee or a parent/guardian
- Using District devices or resources for instant messaging
- Changing device settings and/or background images
- Having food or drinks in open containers around technology devices

Consequences of Misuse

Any negligent or purposeful violation of this Responsible Use Policy may result in an immediate administrative referral and/or loss of technology privilege.

Should the Campus administration, Police department, or Technology department confiscate or otherwise request access to a student’s assigned PISD Equipment for any purposes, including suspicion of misuse or misconduct, any investigation into such suspicion and/or cybersecurity response procedures may result in a loss of data, files, or other information stored on that PISD Equipment due to a wipe clean and reset of the device. Students are responsible for saving their data to their cloud-based PISD Google Drive. Students understand and assume the risk of such loss when using PISD Equipment. To avoid the possibility of such loss, Students should use PISD Equipment in compliance with this Responsible Use Policy and should save any such data on their cloud-based PISD Google Drive, rather than on a device’s local drive.

Consequences may include:

- A warning
- In-class consequences
- School-based consequences
- Parent or Legal Guardian contact
- Administration referral
- Loss of device or network access for an extended period of time
- Disciplinary Alternative Education Placement (DAEP)

Technology Student/Parent Policy Agreement

Students - As users of PISD technology, devices, and the PISD wired and wireless networks, students are responsible for reading and abiding by this policy. As a student in PISD, you attest that you have read this Responsible Use Policy, understand the PISD policies relating to responsible use of PISD technology systems and the internet, and agree to abide by these policies. Any violation of this or any District policy may result in disciplinary consequences.

Parents or Guardians - As the parent or guardian of this student, you attest that you have read this Responsible Use Policy relating to the use of the District's technology systems, devices, and the internet. You understand that access to technology is for educational purposes only. While PISD has taken precautions to filter/eliminate controversial materials while students are on its campuses, you recognize it is impossible for the District to restrict all access to materials, and you will not hold PISD or its employees liable for material accessed or acquired by your student or others on the internet. Furthermore, you agree to supervise and monitor your student's technology usage when your student is not in a school setting.

By digitally signing, you allow your student to use PISD equipment, technology, devices, and services, as well as the PISD wired and wireless networks. You and your student agree to follow this policy in its entirety.