Prosper ISD
Employee Responsible Use Policy
Overview

It is the policy of Prosper ISD to maintain an environment that promotes ethical and responsible conduct with all electronic resources and activities. This privilege and extraordinary opportunity to use district resources comes with a responsibility for the employee.

When signing the Prosper ISD Responsible Use Policy, you, as a Prosper ISD employee, are acknowledging that you understand, accept, and agree to abide by the information and requirements outlined in this document:

Prosper ISD employees understand and agree that:

1. Prosper ISD reserves the right to restrict access to technology at any time.
2. The use of Prosper ISD equipment (“PISD Equipment”) and associated technology is a privilege, not a right.
3. There is no expectation of privacy for Prosper ISD employees when using Prosper ISD technology resources. All files stored on PISD Equipment, the District’s network, and/or the cloud are subject to review and monitoring.
4. The terms “equipment” and “device” 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 Prosper ISD.
5. Prosper ISD retains ownership and control of any and all of its hardware, software, equipment, data, documents, or supplies placed in an Alternative Work Site in connection with an authorized telework 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 Prosper ISD’s possession, custody, and control upon termination of an authorized telework arrangement, or upon request by Prosper ISD at any time.
6. If any other PISD Equipment is needed at an Alternative Work Site, employees must send a request to the Technology Department administrators.
7. Employees are not permitted to take designated work location devices other than their assigned laptop (such as a document camera, monitors, printers, etc. used in the performance of job responsibilities) home without prior written authorization from the Technology Department. If an employee is given permission to take a District device home, employees are held to the same District Responsible Use Policy.
8. The terms “software” or “services” refer to any applications or tools, internal or online, provided by Prosper ISD. Software or services licensed by the District are the property of Prosper ISD.
9. Any digital product created by employees in performance of their duties using PISD Equipment, devices, software, and/or services, or while employees are at work, is the property of Prosper ISD.
10. If a tool, web app, app, or other software program is not on the approved software list, staff members must submit a request through Laserfiche’s “Tech Software Request” to be considered for approval.
11. Employees must comply at all times with the Prosper ISD Responsible Use Policy when using devices or digital resources provided by Prosper ISD, or when using their own devices on school property, or at school-related events.

12. Employees must follow Prosper ISD security precautions, such as keeping their username, password, and pictographs confidential at all times.

13. If an employee believes that his/her username, password, or pictograph have been compromised in any way, the employee must contact the Technology Department immediately to assess the situation.

14. Employees agree to adhere to the standards set forth in the Confidentiality Agreement by treating any Prosper ISD business-related information including, but not limited to, student education records, staff personnel records, student or staff medical records, network or computer security information, student or staff network or computer activity information as confidential.

15. All rules and guidelines for District-provided devices, services, and accounts are in effect at all times, whether at or away from the designated work location.

16. All employees must adhere to all school, district, local, state and federal laws, regulations, and guidelines.

17. Employees are required to keep equipment in good, working condition without alterations, markings, or damage of any kind.

18. Employees are expected to report any accidental or non-accidental damage to their device or associated accessories to a supervisor or campus technician immediately.

19. Employees who identify or know of a security problem related to District technology are expected to convey the details to their supervisors or Technology Department immediately without discussing the problem with other employees.

20. If employees discover information, images, messages or behaviors that are inappropriate, dangerous, threatening, or makes them feel uncomfortable, they should immediately report what they observed to a supervisor.

21. Employees are prohibited from using Prosper ISD resources at school, home, or any location to harass other employees or anyone else.

22. Employees may not use any Prosper ISD or personal resources, at work or at home, to maliciously hack, to introduce viruses or other malware, or to manipulate or modify the files of other employees without permission.

23. All employees are expected to follow existing copyright law (Title 17, USC) and educational fair use policies.

24. Employees may only log in using their District-assigned username. Employees must not share their passwords, pictographs, or employee ID numbers with other employees.

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

**Bring Your Own Device (BYOD)**
BYOD technology is defined as technology used at school, but not owned by Prosper ISD. All employees, whether using District technology or their own technology, are expected to follow the District’s Responsible Use Policy.

While at work, employees may bring and use their personal cell phones, laptops, or tablets only (no printers, scanners, televisions, or other electronic devices). BYOD is a privilege, not a right, and inappropriate use may result in cancellation of that privilege. The following guidelines must be followed by employees using a personally-owned electronic device at work.

1. Administrators and the Technology Department have the right to prohibit employees from using video, photographic, or audio recording on their personal devices, including phones and smart watches, or to restrict the use of any app or feature as deemed necessary for the purposes of privacy, safety, and instruction.
2. Devices operated by employees at work must utilize the Prosper ISD-Wireless network.
3. Employees may not interfere with or circumvent the Prosper ISD-Wireless network by using personal networking devices, or software such as wifi hotspots, access points, routers, etc., which could disrupt PISD Equipment and/or services due to the introduction of malware or the use of malicious websites.
4. Use of Prosper ISD-Wireless through personally-owned devices is primarily intended for instructional use. Prosper ISD-Wireless may be shut down entirely to safeguard the integrity of the network, protect employees from malware or malicious actors, or ensure the functioning of Prosper ISD owned devices and services.
5. Employees are responsible for their own devices. Prosper ISD will not be responsible for the replacement or repair of any personal device which is damaged or stolen while on District property. Any data and/or SMS/MMS (texting) charges will not be reimbursed by Prosper ISD.
6. Employees 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.
7. Employees are not permitted to diagnose, repair, or work on a student’s personal device.
8. Employees are prohibited from engaging in e-commerce using their own device(s) while in Prosper ISD facilities.

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 new 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. Employee 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 Prosper ISD network is a privilege, administrators
may review files and messages to maintain system integrity and ensure that employees are acting responsibly. When Prosper ISD devices are used at other locations, employees must monitor the content accessed on the device.

**Stolen Equipment**

If District-owned equipment is stolen, an employee must contact a supervisor who will initiate a Prosper ISD 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:*

- Any use of technology resources that is deemed disruptive
- Revealing the personally identifiable information\(^1\) 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, pictographs, or providing a student or another employee access to your account, password, or pictograph
- Using the District’s network for illegal activities, including copyright violation, software license or service contract violations, or illegally downloading music, games, images, videos, or other media
- Vandalizing and/or tampering with equipment, programs, files, software, network performance, or other components of the District’s network
- Unauthorized alteration, tampering, copying, 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 or deletion of data stored within District-owned 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 unauthorized activity on the District’s network
- Posting anonymous messages or unlawful information on the District’s network
- Obtaining data or passwords belonging to others on the District’s network
- Placing a computer virus or other malware on a PISD Equipment or the District’s network
- Attempting to access blocked sites, bypassing the internet filter, or concealing internet activity
- Unauthorized downloading or installation of any software, including shareware and freeware
- Using District devices and services for financial or commercial gain, advertising, or political action, activities, or lobbying
- Off-task accessing or exploring online locations or materials that do not support work responsibilities
- Participating in any cyberbullying and/or harassment

\(^1\) "Personally Identifiable Information (PII) | Protecting Student Privacy."
● Using inappropriate language, sexting, sending or accessing pornographic content, sending or accessing sexually inappropriate images, content, or materials, or receiving such materials
● Having food or drinks in open containers around technology devices

Consequences of Misuse

Employees 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. Employees with questions about computer use and data management can contact the Chief Technology Officer.