Prosper ISD

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 user.

When signing the Prosper ISD Responsible Use Policy, you, as a Prosper ISD employee, partner, or other permitted user of Prosper ISD electronic resources and equipment ("User"), are acknowledging that you understand, accept, and agree to abide by the information and requirements outlined in this document:

Users 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 Users 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, Users must send a request to the Technology Department administrators.
7. Users are not permitted to take designated work or placement location devices other than their assigned laptop (such as a document camera, monitors, printers, 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, Users 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 Users 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, unless otherwise stated in writing mutually agreed upon by User and the District.
10. If a tool, web app, app, or other software program is not on the approved software list, staff members must submit a request, "Tech Software Request", through Laserfiche to be considered for approval.
11. Users must comply at all times with the Prosper ISD Responsible Use Policy when using devices or digital resources provided by Prosper ISD. Users must also comply with the Prosper ISD

Responsible Use Policy when using their own devices on school property, at school-related events, and while performing Prosper ISD duties outside of District facilities, such as at trainings, conferences, and telework settings.

12. Users must follow Prosper ISD security precautions, such as keeping their username and password, and pictographs confidential at all times.
13. Users should not use their PISD username or email address when signing up for services unrelated to official PISD business.
14. By employing best cyber security practices, Users should not use their PISD password or any iterations of their password when signing up for any services. This includes services that may be used for official PISD business and those approved by Curriculum and Instruction.
15. If a User believes that his/her username and/or password, or pictograph have been compromised in any way, the User must contact the Technology Department immediately to assess the situation.
16. 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.
17. Users agree to adhere to the standards set forth in the Confidentiality Agreement by treating any Prosper ISD 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.
18. Users shall also comply with Board Policy FL, including all requirements related to access and disclosure. Per Board Policy FL, school officials shall only access student records for which they have a legitimate educational interest.
19. Users must not transmit or publish personally identifiable information (PII) such as social security numbers or passwords via unsecured methods such as email or texting. Encrypted email or other secured means of document transfer should be used instead.
20. Users should never store sensitive data in unapproved areas. All sensitive data must remain accessible only on officially designated systems or in-network storage locations specifically created by district leadership for such purposes.
21. 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.
22. All Users must adhere to all school, district, local, state and federal laws, regulations, and guidelines.
23. Users are required to keep equipment in good, working condition without alterations, markings, or damage of any kind.
24. Users are expected to report any accidental or non-accidental damage to their device or associated accessories to a supervisor or campus technician immediately.
25. Users 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.
26. If Users 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.

27. Users are prohibited from using Prosper ISD resources at school, home, or any location to harass other Users or anyone else.
28. Users 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 Users without permission.
29. All Users are expected to follow existing copyright law *(Title 17,USC)* and educational fair use policies.
30. Users may only log in using their District-assigned username. Users must not share their passwords, pictographs, or employee ID numbers (when applicable) with other Users.
31. 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 Users, whether using District technology or their own technology, are expected to follow the District's Responsible Use Policy.

While at work or placement in Prosper ISD, Users 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 Users using a personally-owned electronic device at work or placement in Prosper ISD.

1. Administrators and the Technology Department have the right to prohibit Users 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. Users may not interfere with or circumvent the Prosper ISD-Wireless network by using personal networking devices, or software such as Wi-Fi 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.
3. 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 Users from malware or malicious actors, or ensure the functioning of Prosper ISD owned devices and services.
4. Users 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.
5. Users are responsible for their device setup, maintenance, and charging. Users will not store a student's device, unless the device was taken up as a disciplinary action or for testing.
6. Users are not permitted to diagnose, repair, or work on a student's personal device.
7. Users are prohibited from engaging in e-commerce using their own device(s) while in Prosper ISD facilities.

8. Users are prohibited from accessing, receiving, or distributing pornographic content and sexually explicit images, websites, content, or materials using a personal device and/or personal cellular network while inside 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. 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 Prosper ISD network is a privilege, administrators may review files and messages to maintain system integrity and ensure that Users are acting responsibly. When Prosper ISD 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 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, User, 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 User or student by using their account, password, pictographs, or providing a student or another User 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

[1] "Personally Identifiable Information (PII) | Protecting Student Privacy." https://employeeprivacy.ed.gov/content/personally-identifiable-information-pii Accessed 2 April. 2019.

- 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
- Using inappropriate language, sexting, sending or accessing pornographic content, sending or accessing sexually explicit images, websites, content, or materials, or receiving such materials
- Having food or drinks in open containers around technology devices

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.