Acceptable Use Policy for Employees

Electronic Network, Internet and Technology Equipment Access Peru Elementary School District 124

Updated 7-16-25

Statement of Understanding and Authorization

The use of the District's technology and electronic networks is an integral part of an employee's work responsibilities in the District. Therefore, each employee ("user") must sign the Peru Elementary School District 124 Acceptable Use Policy Statement of Understanding and Authorization as a condition for using the electronic network, Internet and technology equipment throughout the District. The signature is legally binding and indicates the user has read and fully understands the terms and conditions of this policy and shall be included in the employee's personnel file.

1. Introduction

All user access and use of the electronic network, Internet and technology equipment must be consistent with the District's goal of promoting educational excellence and contributing to the efficient management of district business. This policy is intended to cover all available school technologies, including but not limited to networks, Wi-Fi, computers, mobile devices, email, the cloud, the Internet and similar equipment, networks and access. This may include the use of personally-owned devices on the school campus. These user guidelines extend beyond the school district's physical building, such as school-issued email accounts, hardware, or software used when off the school district's property.

2. Usage Guidelines

A. **Acceptable Use-** Access to the electronic network must be for the purpose of education and research related to school curriculum, assignments and/or assessments, and for the efficient management of district business. All use must also be consistent with Board of Education Policy, as well as the District's educational goals and objectives.

B. **Privileges-** The use of the electronic network is a privilege and not a right. Inappropriate use may result in the loss of privileges, disciplinary action, and/or appropriate legal action.

C. **Unacceptable Use-** The user is responsible for his or her actions and activities involving the network. The following list serves as examples of unacceptable uses however this list should not be considered exhaustive:

1. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law. This includes, but is not limited to, "hacking," cyberstalking, unauthorized tampering with computer systems, using misleading domain names, identity fraud, and engaging in plagiarism (using other's words or ideas as your own)
2. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused.

3. Downloading of copyrighted material for other than personal use. Users should assume that all materials available on the Internet are protected by copyright unless explicitly indicated otherwise.
4. Using the network for private financial or commercial gain.
5. Wastefully using resources, such as file space.
6. Hacking or gaining unauthorized access to files, resources, or entities.
7. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature including a photograph.
8. Using another user's account or password or allowing others access to District-owned devices and equipment. Do not impersonate, spoof, or otherwise pretend to be someone else online. This includes, but is not limited to, sending out email, creating accounts, or posting messages or other online content (e.g. text, images, audio, or video) in someone else's name.
9. Posting material authored or created by another without his/her consent.
10. Posting anonymous messages.
11. Using the network for commercial or private advertising.
12. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, discriminatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material, or is in any violation of any Board policy regarding misconduct, including but not limited to bullying, intimidation, harassment or threats.
13. Using the network while access privileges are suspended or revoked.
14. Using encrypted communication without prior approval.
15. Deleting data, hiding, or attempting to interfere with the discovery of a violation of this policy.
16. Attempting to bypass security settings or Internet filters or interfering with the operation of the network, including other devices connected to the network. Software designed to do so is prohibited on the network. Such software includes but is not limited to file sharing, VPN tunnels, port scanners, DDOS, or malware software.
17. Installation of unauthorized software, browser extensions, unapproved games, and or shareware on school computers.

Any and all communication with students via social media, text messaging services or other means that negatively impacts any student, the school District or its reputation, the reputation of its employees, or its educational interests, or that may negatively impact the school community at large is strictly prohibited. Such activity, even if engaged in on an employee's own time and off school grounds, may result in discipline up to and including termination of employment.

4. Network Etiquette- The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following

A. Be polite.
B. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
C. Do not reveal personal information, including the addresses or telephone numbers or social media accounts of the user, students or other people. It is unsafe and not recommended to post any personal information about oneself or others online, including but not limited to name,

address, phone number, or school. Do not post photos of others with their first and last names on any online site, including but not limited to blogs, wikis, and discussions forums.

D. Recognize that email and social media accounts are not private. People who operate the system have access to all email [6D, 10A, 21]. Messages relating to or in support of illegal activities may be reported to the authorities.
E. Do not use the network in any way that would disrupt its use by other users.
F. Consider all communications and information of other people to be private property.

5. No Warranties- The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District does not guarantee user privacy or system reliability. The District will assume no responsibility for any damages the user suffers, including when his or her device is connected to the District's network. This includes the maintenance, damage, loss, repair, or replacement of personal equipment or data stored on the District network or storage devices. This also includes loss or corruption of data resulting from delays, non-deliveries, missed deliveries or service interruptions. Use of any information obtained via the Internet is at the user's own risk. The District is not responsible for the accuracy or quality of information obtained through its services or Internet. The District does not take responsibility for any information that may be lost, damaged, altered, or unavailable when using its services or the Internet. The District assumes no responsibility for damage, loss, or theft of devices a student brings to school.

6. Indemnification- The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of this policy, including such incurred through copyright violation, or damage to personal equipment or data.

7. Security- Network security is a high priority. If the user can identify a security problem in the network or on the Internet, the user must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Users are required to use two-factor authentication on all Google Workspace devices and applications, and wherever else two-factor authentication is implemented. Do not use another individual's account without written permission from that individual. Attempts to log on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network and may face other disciplinary actions.

8. Vandalism- Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy the data of another user, the Internet, District web page, social media accounts, or any other network. This includes, but is not limited to, uploading or creating computer viruses and or tampering with computer systems.

9. Responsibility for Costs Incurred- The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, social media or application charges, download fees, bandwidth use and/or equipment or line costs. Any and all such unauthorized charges or fees shall be the responsibility of the user.

10. Copyright Web Publishing Rules- Copyright law and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers without explicit written

permission. Users should assume that all materials available on the Internet are protected by copyright unless explicitly stated otherwise.

A. For each re-publication of a graphic or a text file on a website, file server social media account or other that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.
B. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission in written form. The manager of the website displaying the material may not be considered a source of permission [9B].

11. Use of Email- The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides email to aid users as a tool that is to be used for educational purposes only.

A. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any user to an email account is strictly prohibited.
B. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
C. Electronic messages transmitted via the District's Internet gateway carry with them an identification of the user's Internet domain. This domain is a registered name and identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
D. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the appropriate administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
E. Use of the District's email system constitutes consent to these regulations.
F. District and building administrators utilize e-mail as the primary mode of written communication with staff. It is expected that all staff regularly access e-mail accounts provided by the school district. Staff members leaving the district will have their accounts disabled as of their final contract day unless other arrangements are made.
G. Along with their name, position and basic contact information, employees shall include the following statement in the signature of their e-mail account: *This email and any files transmitted with it may contain confidential and legally privileged information. It is intended solely for the addressee(s). If you are not the intended recipient, you may not disclose, copy, distribute, read or use any of this information. If you received this communication in error, please contact the sender immediately, permanently delete this email from your system and destroy any hard copy of this or any related files.*

12. Internet Safety

A. Internet access is limited to only those acceptable uses as detailed in these procedures. Users may not engage in unacceptable uses, as detailed in these procedures [1].
B. To ensure that the users abide by the terms and conditions for Internet access contained in this policy, the District will provide for the education of students about appropriate online behavior, including interacting with other individuals on social networking and cyberbullying awareness and response.
C. The District provides Internet filtering that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act (CIPA). While the District may employ filters to limit access to certain kinds of sites and to prevent unwanted or inappropriate materials from being accessed or transmitted, there is no guarantee that all objectionable material will be caught or filtered. Limiting this kind of materials is the joint responsibility of all users accessing the District's network.
D. An administrator or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the user receives prior permission from the Superintendent or designee.

13. Off Campus Computer Use- All provisions of this policy apply to the use of any home-based or off-campus computer or other personal or district-owned device which is used to conduct District business or communications. This includes school-issued email accounts, hardware, or software used when off the school district's property. All District-owned devices, regardless of physical location (in and out of school), will have Internet activity protected and monitored.

14. Mobile Device Policy- The District may provide students or employees with mobile computers or other devices to promote learning outside of the classroom. Users must abide by this policy when using school devices outside of the school network. Users are expected to treat these devices with extreme care and caution. Users should immediately report any loss, damage, or malfunction to the Building Principal or appropriate staff. Users may be financially responsible for any damage resulting from negligence or misuse. Use of school-issued devices off the school network may be monitored.

15. Authorization for Network Access- No unauthorized equipment will be allowed on the network. Permission must be granted by the appropriate school personnel before outside devices are allowed on the network. Any employees or guests who need access to the network must seek permission from the office and then authorized personnel will put in the password.

16. Social Media and Text Messaging Services- The District may provide access to social media, text messaging services, blogs, Internet forums, wikis or similar online networks for the purpose of educational needs. With prior permission of the Superintendent or his or her designee, social media sites may be accessed only for educational and school related purposes, in connection with lessons and assignments to facilitate communication with teachers and students. Passwords for such site(s) must be shared with the appropriate administrator.

An employee shall be responsible for all content posted or uploaded to any social media site. Employees are prohibited from posting any confidential information regarding students or staff. No photos of students may be posted without parental permission. Staff should not permit students to

upload or post information or photographs without direct supervision. Web-based applications where the public can post or respond must be monitored on a daily basis, and posts about a student or staff member that violate the inappropriate usage policy must be removed.

Employees must allow parents the opportunity to "opt-out" of their child receiving communications or messages from a staff member. If a student or parent refuses to accept messages from an employee, the school District employee must use an alternative means of communication without any penalty to the student involved.

The content of all text or similar messages must directly involve a school-related subject matter. Cell phone texting should never be used to conduct a personal conversation with a student. If an employee receives an inappropriate text message from a student, it is the responsibility of that employee to contact a student's parent and school administration immediately to address the situation as appropriate.

As stated under the "Unacceptable Use" section above, any and all communication with students via social media, text messaging services or other means that negatively impacts any student, the school District or its reputation, the reputation of its employees, or its educational interests, or that may negatively impact the school community at large is strictly prohibited. Such activity, even if engaged in on an employee's own time and off school grounds, may result in discipline up to and including termination of employment.

17. Due Process- The District will cooperate fully with local, state, or federal officials in any investigation correlating to any illegal activities conducted through the District's network. In the event there is an allegation that a user has violated the District Acceptable Use Policy, the person will be provided with a notice and opportunity to be heard in the manner set forth according to Board policy.

18. No Expectation of Privacy- Users have a limited expectation of privacy with regard to the contents of their network files, and online and/or network activity may be monitored at any time. Software may be used to monitor computer usage, system information, and remotely observe and manage network technology. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the District Acceptable Use Policy or other District policies. All messages sent to or received from students on school District issued technology are the property of the school District. Relevant messages sent via text or other messaging services may be reviewed by District personnel at any time and may be recorded for District purposes. All content posted to social media or sent via text or other messaging services may also be subject to public records laws as applicable.

Acceptable Use Policy for Employees
Statement of Understanding and Authorization
Electronic Network, Internet and Technology Equipment Access
Peru Elementary School District 124

Updated 7-16-2025

In accordance with Board of Education Policy 6:235, on an annual basis each employee and user must sign the Statement of Understanding and Authorization to be allowed to use the Internet and the District's electronic network and technology equipment in accordance with all provisions of the District Technology Acceptable Use Policy.

The signature is legally binding and indicates the user has read and fully understands the terms and conditions of this policy. The user understands that the failure of any user to follow these policies will result in the loss of privileges, disciplinary action, and/or appropriate legal action, and that the District has taken precautions to eliminate controversial material.

By signing the Statement of Understanding, the user agrees to release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, inability or failure to properly use the District's electronic network, Internet and technology equipment as outlined in the Acceptable Use Policy for Employees.

_____	_____
Employee Name (please print)	Employee Signature
_____	_____
Applicable School Term	Date of Signature