Acceptable Use Policy for Students
Electronic Network, Internet and Technology Equipment Access
Peru Elementary School District 124

Approved 6-15-16

Acceptable Use Policy Statement of Understanding and Authorization

Each student's parent/guardian 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(s) at the end of this document are legally binding and indicates the signer has read and fully understand the terms and conditions of this policy. The failure of any user to follow these policies will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Introduction

All student access and use of the electronic network, Internet and technology equipment must be consistent with the District's goal of promoting educational excellence. 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.

Usage Guidelines

1. 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 must also be consistent with the District's educational goals and objectives.

2. Privileges - The use of the electronic network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges and may also include disciplinary action as outlined in Board of Education policy and the Student Handbook. The Superintendent or designee will make all decisions regarding whether or not a user has violated these procedures and the district may deny, revoke, or suspend student access at any time it deems this to be necessary for the safety and welfare of others.

3. Unacceptable Use - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

A. 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;
B. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
C. Downloading of copyrighted material for other than personal use;
D. Using the network for private financial or commercial gain;
E. Wastefully using resources, such as file space;
F. Hacking or gaining unauthorized access to files, resources, or entities;
G. 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;
H. Using another user's account or password;
I. Posting material authored or created by another without his/her consent;
J. Posting anonymous messages;
K. Using the network for commercial or private advertising;
L. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, 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.

M. Using the network while access privileges are suspended or revoked.
N. Using encrypted communication without prior approval.
O. Deleting data, hiding, or attempting to interfere with the discovery of a violation of this policy.

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, other or other students or people.
D. Recognize that email and social media accounts are not private. People who operate the system have access to all email. 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 will not be responsible for any damages the user suffers. This includes loss 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 specifically denies any responsibility for the accuracy or quality of information obtained through its services or Internet. Further, the District does not take any responsibility for any information that may be lost, damaged, altered or unavailable when using its services or the Internet.

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.

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. 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 or social media accounts, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

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.

A. For each re-publication of a graphic or a text file on a website, file server socal 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.

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 students 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 student 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 system 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.

12. Internet Safety

A. Internet access is limited to only those acceptable uses as detailed in these procedures. Students may not engage in unacceptable uses, as detailed in these procedures.
B. To ensure that the students 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. 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 material 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 person receives prior permission from the Superintendent or designee.

13. Off Campus Computer Use

Using a home-based or off-campus computer such that the use results in material and/or substantial disruption and/or threat at or to the school will constitute grounds to investigate whether the use violates applicable law or school rules. Should such misuse be determined, the student may receive disciplinary consequences appropriate for the frequency and severity of the violation.

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 mobile devices off the school network may be monitored.

15. Social Media

The District may provide access to social media, blogs, Internet forums, wikis or similar online networks for the purpose of educational needs. Examples of social media include, but are not limited to, Facebook, Twitter, YouTube and Google+. Social media sites must be used only for educational and school related purposes, in connection with lessons and assignments to facilitate communication with teachers and other students.

16. 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.

17. No Expectation of Privacy

Students have a limited expectation of privacy with regard to the contents of their network files, and online and/or network activity may be monitored while using the District's network. 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.

Statement of Understanding and Authorization

On an annual basis, each student's parent/guardian must request through the Student Handbook Statement of Understanding that his/her child 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 as found in the Student Handbook.

The signature is legally binding and indicates the parent has read and fully understand the terms and conditions of this policy. The student's parent/guardian 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 student's parent/guardian agrees to release the School District and its Board members, employees, and agents from any claims and damages arising from the use of, or inability to use the District's electronic network, Internet and technology equipment, accepts full responsibility for supervision if and when his/her child's use is not in a school setting, and agrees to discuss the Acceptable Use Policy with his/her child.