

POST FALLS SCHOOL DISTRICT NO. 273

Series 600: Non-Certified Personnel: Related Considerations

Policy No. 604.8

Policy Title: Employee Computer and Network Service

Page 1 of 4

The Board of Trustees of Post Falls School District #273 recognizes the importance of using current technologies in the schools as part of a planned program to prepare students for a technological society. The board recognizes the establishment of computer networks with internet access for instructional and administrative use. The district's goal in providing this service is to promote educational excellence in schools by facilitation of resource sharing, innovation, and communication.

Privileges and Responsibilities

The use of the district's computer networking capabilities is a privilege, not a right. Use of the district's computer networking capabilities should be related to the classroom curriculum or the staff member's job responsibilities and/or educational issues consistent with the instructional objectives of this district.

Freedom of speech and access to information on the network will be honored; however, the district reserves the right to monitor and review all electronic transmissions and activities. Access may be denied, revoked, or suspended to specific users due to violation of this policy or inappropriate use. Further disciplinary action may also occur.

The Internet/Network Acceptable Use Form is available in the following locations: Skyward Returning Student registration process in digital form, registration packet at all secondary schools, and on the district website. Students and staff are expected to accept and follow the rules and regulations concerning acceptable use.

The public will be provided information regarding internet use rules and regulations through district policy (found on our website), newsletters, and student handbooks.

Information Content

The district prohibits the use of school computers and other school technology devices from sending, receiving, viewing, or downloading materials that are deemed harmful to minors. The district will continue to implement filtering and blocking measures to prevent access to and by students and staff from restricted websites and e-mail.

The computer network services provided by the district may not always be uninterrupted or error-free. They are provided on an "as-is, as-available" basis. The district makes no warranties with respect to any service and any information or software contained therein.

Opinions, advice, services, and other information expressed by students, staff, information providers, service providers, or other third parties on the computer network service provided by the district are those of the individual and do not necessarily represent the position of the district. All school policies and rules pertaining to behavior and communications apply.

The following uses of the district's computer system, including the internet, are strictly prohibited. Violations are cause for disciplinary action.

1. Using the network for political or commercial purposes.
2. Offering for sale any goods or services that could be construed as a commercial or private enterprise, unless approved by the board or designee.
3. Using the network for any illegal activity including violation of copyrights, trade secrets or other contracts, or transmitting any materials, information, software in violation of federal or state laws.
4. Using the network to send, receive, or access any defamatory, inaccurate, abusive, obscene, profane, pornographically and sexually oriented, threatening, harassing, objectionable, or illegal

material, or material which may encourage the use of controlled substances.

5. Using the network for destructive purposes (destroying or damaging property directly or via viruses), or to infiltrate a computing system and/or damage the software components, or gain unauthorized access to any network or database.
6. Using the network to send/receive messages that are inconsistent with the district's code of conduct.
7. Using, or attempting to use, another user's account, password, or credentials.
8. Misrepresenting the identity of the sender of messages or posting anonymous messages.
9. Using the network while access privileges are suspended or revoked.
10. Vandalism of the district's computer. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the computer network service, or any of the agencies or other computer network services that are connected to the internet. Vandalism includes, but is not limited to, the uploading or creation of computer viruses.
11. Connecting personal computing devices to the district's network.
12. Accessing information from outside the district, whether stored directly on district servers or on servers outside the district contracted to house information.
13. Using any type of device, application, or service designed to bypass district filtering or security settings.

Employees should only use the network for non-school matters during their non-work time. As always, all use of the network must conform to this policy.

Electronic Mail

Electronic mail (e-mail) is a private electronic message sent by or to a user in correspondence with another person having internet mail access. The following provisions apply to e-mail:

1. It should be recognized by users that e-mail may be viewed by others. Within a public school district, e-mail may be considered public information. There is no guarantee of confidentiality.
2. The district administrators will not intentionally inspect the contents of e-mail sent to an intended recipient, or disclose such contents to anyone other than the sender or an intended recipient, without the consent of the sender or an intended recipient. However, such inspection or disclosure may occur if it is required by law or district policies, or to investigate allegations that the e-mail may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive, or illegal material.
3. E-mail messages may be subject to public inspection through public records requests.
4. Users are not to download or forward e-mail messages that have originally been sent from an unknown source.

Employee Use of Social Media Technology and Electronic Communication

Social media technology can serve as a powerful tool to enhance education, communication, and learning. This technology, when used appropriately, can provide both educational and professional benefits, including preparing students to succeed in their educational and career endeavors. Social media is defined as any form of online publication or presence that allows interactive communication, including, but not limited to: social networks, blogs, internet websites, internet forums, and wikis. Examples of social media include but are not limited to: Facebook, Twitter, YouTube, Instagram, Snapchat, etc.

Employee Use of Social Media Sites, Including Personal Sites

Due to the unique nature of social media and the district's desire to protect its interest with regard to its electronic records, the following policies have been established to address social media site usage by all employees.

Protect Confidential and Proprietary Information

Employees shall not post confidential or proprietary information about the district, its employees, students, agents, or others. The employee shall adhere to all applicable privacy and confidentiality policies adopted by the district or as provided by state or federal law. Employees shall not use images of students, or names or data relating to students, absent written authority of the parent of a minor or authority of an adult or emancipated student.

At no time shall employees store confidential or proprietary information about the district, its employees, students, agents, or others on personal devices or accounts.

Use of the District's Name, Logos, or Images

Employees shall not use the district logos, images, iconography, etc. on personal social media sites. Nor shall employees use the district name to promote a product, cause, political party, or political candidate.

Respect District Time and Property

Employees shall not use district technology for personal e-mail, text messaging, and social media. Employees should refrain from the aforementioned activities for personal purposes except during non-designated work times and should use his/her personal device. Any use must occur during times and places where the use will not interfere with job duties, negatively impact job performance, or otherwise be disruptive to the school environment or its operation.

On Personal Sites

Individuals identifying themselves as district employees must state that the views expressed, posted, or published are personal views, not necessarily those of the district, the board, employees, or agents. Opinions expressed by employees on a social networking website have the potential to be disseminated far beyond the speaker's desire or intention, and could undermine the public perception of fitness of the individual and district to educate students, and thus undermine the teaching effectiveness. In this way, the effect of the expression and publication of such opinions could potentially lead to disciplinary action being taken against the employee, up to and including termination or nonrenewal of the contract of employment.

Keep Personal and Professional Accounts Separate

Employees who choose to engage in professional social media activities will maintain separate professional and personal e-mail addresses. Employees will not use district e-mail for personal social media activities. Use of district e-mail for this purpose is prohibited and will be considered a violation of district policy that may result in disciplinary action.

Contact with Students

Although it is desired that employees have a sincere interest in students as individuals, partiality and the appearance of impropriety must be avoided. Pursuant to the Code of Ethics for Idaho Professional Educators, individuals shall maintain a professional relationship with all students, both inside and outside of the classroom and will adhere to each of the following:

1. Employees should not have online interactions with students of the district on social networking sites outside of approved forums dedicated to academic use. Listing current students as "friends" on networking sites is prohibited. District employees' social networking profiles and personal blogs should not be linked to district students' online profiles in any manner.
2. Employees should not contact students of the district through electronic means other than the district's e-mail, telephone system, or academic forum (i.e. School Messenger) unless such communication includes the parent(s)/ guardian.
3. Athletic or academic coaches, advisors, or other student group leaders, or designee approved by the building administrator shall not electronically contact a team member or members without including all team members in the communication, unless such communication includes the parent/guardian and/or his her supervisor.

4. Employees shall not have inappropriate contact of any kind with students including via electronic media.

Nothing in this policy prohibits employees and students from the use of educational websites or the use of social networking websites created for curricular, co-curricular, or extra-curricular purposes where the professional relationship is maintained with all students. Failure to maintain a professional relationship with students will result in disciplinary action.

Complaint Procedure

1. Complaints from staff will initially be taken to the building principal and will follow the chain of command. Complaints will be reviewed in a manner which promotes a thorough, orderly, and fair evaluation providing for expeditious resolution of the problem.
2. Complaints by students, their parents, or patrons regarding any rule or regulation pertaining to computer and Internet use will follow the established chain of command pursuant to Policy 206.3a, Patron/Student Complaint.
3. The board encourages orderly and timely resolution of complaints. It is the wish of the board and the district administration that every effort be made to resolve complaints in an information manner that is conducive to positive communication and relations for all parties.

Disciplinary Action

Violation of any part of this policy may result in the following disciplinary actions:

1. When an employee violates this policy, his/her computer privileges/network access may be restricted, suspended, or terminated by the building principal or supervisor. Flagrant violations, or a pattern of persistent violations, may result in further disciplinary action, up to and including termination of employment for employees and suspension for students.
2. Users whose conduct is reasonably considered to be illegal, as defined by federal and/or state law, will be referred to local law enforcement for prosecution.
3. Each user will be held responsible for any damage he/she causes to district's computers or to the computer network service and may be required to pay all costs incurred in restoring the computer or network service to its previous working order.

Any action by a user that is determined to constitute an inappropriate use of the district's computer network service or to improperly restrict or inhibit other users from using and enjoying the district's computer network service is strictly prohibited and may result in disciplinary action.

Legal References: 17 USC Section 1001, et seq.
IC§ 6-210, 18-2201, 18-2202, 33-131

Applicable Procedural Regulations: 405.18a

Date of Adoption: 12/11/00

Revised: 9/12/11; 3/8/21

Reviewed: 2021, 2023