Electronic Information System (Network)

Acceptable Computer Use Rules and Regulations

This policy applies to students, employees, and volunteers.

Network

A. Access to the network and Internet resources is recognized by the user as a privilege not a right. Users are responsible for the appropriateness and content of material they create, store, transmit, or publish on the network.

B. The District reserves the right to prioritize use and access to the network. The District further reserves the right to create a social media account on behalf of the District, to be monitored and permitted based on the Superintendent's discretion. Anyone who utilizes the District' social media account must do so consistent with District Policies and Procedures.

C. All computer and telecommunications equipment comprising the network and all information created, sent, or received via this equipment is property of the District (excluding individual copyrighted curriculum material). They are to be used for District purposes in support of education and research and be consistent with the mission of the District.

D. Any use of the system must be in conformity with state and federal law, Charter service provider policies and licenses and District policy. Use of the system for commercial solicitation, financial gain, or any illegal activity is strictly prohibited. Use of the system for charitable purposes must be approved in advance by the superintendent or designee.

. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures. Employees, acting as representatives for a union/employee association, cannot utilize the network to conduct union/employee association business except where agreed upon, in writing, between the District and the union/employee association.

F. Network components including hardware or software shall not be destroyed, modified, or abused in any way. Connecting or installing unauthorized components, i.e.; an employee's personal hardware or software, to the network for any purpose inconsistent with District policy is prohibited, unless prior approval from a site Administrator has been granted.

G. Prior administrative approval must be granted to utilize District equipment offsite and must be in conjunction with District related work.

H. Development or use of malicious programs that harass other users or gain unauthorized access to any computer or computing system and/or damage the components of a computer or computing system is prohibited. No use of the network shall serve to disrupt the operation of the network by others.

I. Any use that is deemed to adversely affect the District, students or its employees, including, but not limited to: hate mail, harassment, discriminatory remarks, or other antisocial behaviors is expressly prohibited and is a violation of **WAC 181-87-060 Disregard or abandonment of generally recognized professional standards.**

. Use of the system to access, transmit, store, display, distribute, or request obscene, pornographic, erotic, profane, racist, sexist, or other offensive material (including messages, images, video, or sound) that violates District policies or creates a hostile work environment is prohibited.

K. Digital content broadcast via the Internet (streaming) including, but not limited to: video, music, news/weather, stock reports, sports information, is supported when used in the context of a course curriculum or is not having a negative impact on network resources. The District reserves the right to shut down or limit these resources during periods of district-wide activities (assessments) when high utilization of network resources is needed.

L. No software (shareware, freeware, trial-based, utilities, pirated, etc.) shall be downloaded and installed on District computers without permission of the Information Technology Department or building administrator.

Security

A. System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users should not share their account ID's or passwords with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.

B. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to the system.

C. Communications may not be encrypted so as to avoid security review.

D. Personal information such as addresses, telephone numbers, SSN, Driver's License numbers, etc. of employees and students should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher or other building representative. Such information should only be disseminated on a need to know basis.

E. Due to the un-secure nature and threat of security breach, use of Internet chat rooms, chat channels, Internet Chat Relay (IRC) programs, or 3rd-party (Microsoft, AIM, Yahoo) Instant Messaging (IM) systems for communications purposes is strictly prohibited. The District will provide these resources under certain conditions and only as part of normal business practices.

F. Students should notify their teacher or other building personnel whenever they come across information or messages that are dangerous, inappropriate, or that makes them feel uncomfortable.

Personal Security

A. All users should be aware that any information, software, or graphics on the Internet might be protected by federal copyright laws, regardless of whether a copyright notice appears on the work.

B. The unauthorized installation, use, storage, or distribution of copyrighted Intellectual Property on District computers or using materials in violation of copyright laws, is prohibited.

C. Use of online peer-to-peer (P2P), file sharing, MP3, "Fast Track", or related technologies is prohibited. These technologies are mainly/frequently used to distribute copyrighted works illegally and use of these on District property could result in the District being held liable for copyright infringement. Similarly, access to personal accounts established on these systems, from District property is also prohibited.

Filter and Monitoring

. The Network currently has filters to block or filter out visual depictions that are deemed obscene, pornographic especially child pornography, harmful or harmful to minors. However, every user has the responsibility to prevent and/or immediately report any such occurrence to the Information Technology Department. Failure to do so could result in the loss of access privileges.

B. Education staff will monitor student's use of the Internet in school, and will take reasonable measures to prevent access by students to inappropriate materials on the Internet and the World Wide Web, and restrict their access to materials harmful to minors.

Education

The District will educate minors about the appropriate online behavior. This is to include using electronic mail, chat rooms, and other forms of direct electronic communications. It is critical that students understand the risks associated with unlawful online activities and the disclosure of personal information over the internet.

General Use

A. Diligent effort must be made to conserve system resources. For example, users should frequently delete e-mail and unused files.

B. No staff member shall have access to the system without having received appropriate training and signing an *Electronic Mail and Network Information System User Agreement* (see Appendix C).

C. Users will carefully review all e-mail prior to sending it to ensure that it is consistent with this policy and their meaning is clear and not subject to misinterpretation. Humor and sarcasm can be easily misinterpreted in an e-mail and should be avoided whenever possible.

D. All computers will have anti-virus software installed. This software is to remain activated at all times. Users should follow District recommendations with regard to the safe keeping of data and e-mail attachments to reduce the risk of spreading viruses (worms, viruses, trojan horses, etc.), and infecting computers and the network.

E. Personal use of District systems is authorized within reasonable limits as long as it does not interfere with or conflict District use. Personal use of the Network by employees cannot impact the employee's performance of their job duties. Employees are responsible for exercising good judgment regarding reasonableness of personal use. In case of doubt, consult your immediate Administrator.

F. Parents of students under the age of 18 may choose to have their students "opt out" of having access to the Network. This must be done in writing to the school. It is highly recommended that parents have a conversation with the building administrator prior to initiating this "opt-out" action.

From time-to-time, the District will make a determination of whether specific uses of the system are consistent with the regulations stated above. Under prescribed circumstances non-student or non-staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and mission of the District. For security and administrative purposes, the District reserves the right for authorized personnel to review system use and file content. The District reserves the right to remove a user account on the system to prevent further unauthorized activity.
Violation of any of the conditions of use may be cause for disciplinary action.

PRESCOTT SCHOOL DISTRICT #402-37

doption Date: **12/17/2015**
Classification: **Discretionary**
Revised Dates: **04.98; 12.11; 10.15**

WAC 181-87-060

Disregard or abandonment of generally recognized professional standards.

Any performance of professional practice in flagrant disregard or clear abandonment of generally recognized professional standards in the course of any of the following professional practices is an act of unprofessional conduct:

(1) Assessment, treatment, instruction, or supervision of students.

(2) Employment or evaluation of personnel.

(3) Management of moneys or property.

[06-02-051, recodified as § 181-87-060, filed 12/29/05, effective 1/1/06. Statutory Authority: RCW [illegible]. WSR 90-02-075, § 180-87-060, filed 1/2/90, effective 2/2/90.]