PGISD Network Services Acceptable Use Regulation (AUR)

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

The District will provide training to system users in proper and ethical use of the system and will provide access to this **Acceptable Use Regulation (AUR)**. All system users will agree to abide by the **AUR**, in writing, before access to network services is permitted. The District will provide training to students in proper and ethical use of the system and will provide copies of the **Student Network Responsibility Contract (SNRC)**. All students will agree to abide by the **SNRC** in writing, before access to network services is permitted.

No Expectation of Privacy

Pleasant Grove ISD reserves the right to manage all systems and services, including accessing records, messages, and other files stored on, transmitted via or resulting from the use of these resources. Users should have no expectation of privacy associated with the information they store in, send or receive through the network services systems. The district reserves the right to access and monitor this information without prior notice. No user should have any expectation of privacy as to his or her technology use and all users consent to the monitoring of same. All computer equipment and its contents are the property of the district and subject to review anytime at its discretion.

System Access

1. Access to the District's network services is a privilege, and not a right.
2. Access to the District's network services will be provided to the following if requested by the campus principal or the superintendent:
    a. Employees, excluding substitute teachers
    b. Students
    c. Long term substitute teachers
    d. Student teachers if requested by the supervising teachers
    e. Community volunteers – permissions will be limited and individually specified on the signature sheet
    f. Tech Approved Substitutes (TAS) – permissions will be limited and individually specified on the AUA signature sheet
    g. Parents may access VSI in any campus library under supervision of the librarian
3. Tech Approved Substitutes, wearing the TAS badge may supervise student computer use. Other short term substitute teachers are not allowed access to the network and are not allowed to supervise student access.
4. Vendors, workshop attendees and community volunteers must have permission of the technology director before access to network services, and must sign an **Acceptable Use Regulation (AUR)** with individual permissions and restrictions noted.
5. Access to the District's network services may be denied to any user identified as a security risk or having violated District and/or campus computer use guidelines.

Personal Use

Access to the District's electronic communication system, including the Internet, shall be made available to students, employees and student teachers primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Is not otherwise prohibited by policies, rules or regulations;
3. Does not unduly burden the District's computer or network resources; and
4. Has no adverse effect on a student's, teacher's or employee's job performance or on a student's academic performance.

Consent Requirements

1. Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright.

2. No original work created by any District student will be posted on a Web page under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor) or employee who created the work.
3. No personally identifiable information about a District student will be posted on a Web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Educational Rights and Privacy Act and District policy.

Technology Director Responsibilities

The technology director or designee for the District's electronic communications system will:

1. Be responsible for selecting, implementing and maintaining appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers with Internet access provided by the school.
2. Ensure that all Central Services users of network services annually complete an **AUR**. All such agreements will be maintained in the technology director's office.
3. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
4. Be authorized to monitor or examine all system activities, including e-mail transmissions, as deemed appropriate to ensure system user safety on-line and proper use of the system.
5. Set limits for data storage within the District's system, as needed.
6. Ensure that all network resources are protected against malware and intrusion by unauthorized parties.

Principal Responsibilities

As the campus-level coordinator for network services, the principal will:

1. Ensure that all users of network services annually complete either an **AUR** or **SNRC**. All such agreements will be maintained in the principal's office, with copies sent to the technology director.
2. Be responsible for disseminating and enforcing applicable **AUR** and **SNRC** for the District's network Services, as well as any additional network rules as needed.
3. Ensure that campus system users responsible for supervising student computer use are aware of any students not allowed to use network services, either because a signed **SNRC** is not on file or because of termination of privileges.
4. Ensure that system users supervising students using network services provide training to students under their supervision emphasizing the appropriate use of this resource.
5. Be responsible for establishing rules regarding security of computers using network services and located in office areas.
6. Campus principals must notify the technology director or technology specialist by e-mail to cancel system privileges of system users.

Individual User Responsibilities

The following standards will apply to all users of the District's electronic information/communications systems:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. System use for commercial activities or political lobbying is prohibited.
3. Chat rooms and instant messaging is forbidden by all users. The one exception is that chatting is allowed by non-students using the tool provided with the district email system.
4. Newsgroup use is forbidden to students, but allowed for other system users.
5. E-mail or any other form of personal communication by students is not permitted, unless permission is given by the teacher. The teacher may only give such permission after receiving written permission from the technology director or technology specialist.
6. Accessing e-mail from other than the District provided e-mail account from any district computer is prohibited without written permission from the Technology Director.
7. System users responsible for supervising student network use must provide direct supervision to students in his or her care at all times. Direct supervision is defined as present in the room with the student computer users, with frequent monitoring of student activity.
8. When any classroom computer is logged in, the system user must be present, or the door or workstation locked.

9. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy, regulation, or any state or federal law.
10. No system users may disable, attempt to disable, bypass or attempt to bypass a filtering device on any network services computer without a filter bypass account provided by the Technology Director or a technology specialist.
11. Communications or other data cannot be encrypted so as to avoid security review by system administrators.
12. System users may not use another person's system account without written permission from the technology director or technology specialist. Teachers may, however, log on to any student account as needed.
13. System users may reveal their password to the technology director, technology specialists or technology assistants only. Providing your system password to any other person constitutes a violation of network security and is forbidden. Students, however, must provide their system password to any supervisor when requested.
14. Students may not distribute personal information about themselves or others by means of any network services computer; this includes, but is not limited to, personal addresses and telephone numbers.
15. Students should never make appointments to meet people whom they meet on-line and should report to a teacher or administrator if they receive any request for such a meeting.
16. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designate. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
17. System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages from unknown senders and loading data from unprotected computers.
18. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
19. System users should be mindful that use of school-related e-mail addresses might cause some recipients or other readers of that mail to assume they represent the district or school, whether or not that was the user's intention.
20. System users may not access internet resources that use audio or video streaming without prior written permission from the technology director or technology specialist.
21. System users may not gain unauthorized access to resources or information.
22. System users are forbidden from installing any programs or copyrighted material on any computer connected to PGISD network services. Only the technology director, technology specialist or technology assistant may install programs or copyrighted material.
23. Playing games accessed through the Internet is prohibited. Games used as part of the curriculum are not prohibited as long as the websites used are listed in the teacher's lesson plan.
24. District computers that are used off campus may not be connected to the network until they are sanitized by the Technology Director, or designee.
25. Computers and other hardware devices belonging to students or employees may not be connected to any network device. This rule does not apply to removable media such as floppy discs, compact discs and USB drives. Any additional exceptions must be received from the technology director in writing.
26. System users must take precautions to safeguard confidential information from being viewed by unauthorized persons.

Forgery Prohibited

Forgery or attempted forgery of e-mail messages is prohibited. Attempts to read, delete, copy, or modify the e-mail of other system users or deliberate interference with the ability of other system users to send/receive e-mail, or the use of another person's user ID and/or password is prohibited. E-mail and any other network use may be monitored by a designee of the district at any time.

Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District Policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses, worms, spyware, adware or other destructive programs.

Vandalism as defined above may result in the cancellation of system use privileges and may require restitution for costs associated with system restoration, as well as other appropriate consequences.

Information Content/Third Party Supplied Information

System users should be aware that, despite the District's use of technology protection measures as required by law, use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher. A system user knowingly bringing prohibited materials into the school's electronic environment may be subject to disciplinary action in accordance with District policies.

District Web Site

The District will maintain a District Web site for the purpose of informing employees, students, parents and members of the community of District programs, policies, and practices. Requests for publication of information on the District Web site must be directed to the technology director.

No personally identifiable information regarding a student will be published on a Web site controlled by the District without written permission from the student's parent.

No commercial advertising will be permitted on a Web site controlled by the District without written permission of the superintendent.

Staff, Campus and Extracurricular Organization Web pages

With the approval of either the campus principal or the superintendent, staff, campus and extracurricular organization web pages may be published and linked to the District's site Web pages. Publication is subject to the approval of the technology director. Staff members will be responsible for compliance with District rules in maintaining their pages. Any link from staff, campus, and extracurricular organization Web pages to sites outside the District's computer system must be monitored by the author of such page for inappropriate content including changes in that content over time

Student Web Pages

Web pages created and published by students as a classroom assignment on the district system may not be viewable outside the District's computer system without written permission of the Technology Director.

Network Etiquette

System users are expected to observe the following network etiquette:

1. Be polite and courteous at all times.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.
3. Pretending to be someone else when sending/receiving messages is forbidden.
4. Transmitting obscene messages or pictures is prohibited.
5. Be considerate when sending attachments with e-mail by considering whether the file may be too large to be accommodated by the recipient's system or may be in a format unreadable by the recipient.
6. Revealing personal addresses or telephone numbers of others is prohibited. Revealing your personal address or telephone number is strongly discouraged, and at your own risk.
7. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

Termination/Revocation of Network Services Access

Termination of a system user's access will be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of privileges, or on a future date if so specified in the notice. The District may suspend or revoke a

system user's access to the District's system upon violation of District policy and/or administration regulation regarding acceptable use.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information of software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on, the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

Complaints Regarding Copyright Compliance

The District designates the following employee to receive any complaints that copyrighted material is improperly contained in the District network:

Jim McClurg
Technology Director
8500 North Kings Hwy
Texarkana, Texas 75503
(903) 831-4086 jimmcclurg@pgisd.net

2018-2019

Adopted June 16, 2011

ACCEPTABLE USE REGULATION FOR A NETWORK SERVICES ACCOUNT

I have read the District's **Acceptable Use Regulation** for Network Services and agree to abide by its provisions. I understand that I will be subject to monitoring by district staff to ensure appropriate use and I have no expectation of privacy. In consideration for the privilege of using the District's network services and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from any use of, or inability to use, the system.

Name of system user (printed) _____

Signature of system user _____

Date _____

I have received training on how to access school board policy online and I also understand that I can request a printed copy from PGISD Central Services.

System user initial here _____

Individualized Permissions and Restrictions If Needed