PLEASANT GROVE INDEPENDENT SCHOOL DISTRICT
STUDENT NETWORK RESPONSIBILITY CONTRACT

Please read the following carefully before signing this document. This contract must be signed before network access is given.

Pleasant Grove Independent School District Network Services provides access to the Internet. The Internet is an electronic information and communications system connecting millions of computers all over the world. With access to computers all over the world also comes the availability of some materials that may not be of educational value. PGISD believes that the valuable information available on this worldwide network outweighs the possibility of users procuring material that is not consistent with the educational goals of the district.

Here are some of the guidelines establishing the responsibilities you are about to acquire. If any student violates any of these provisions, his or her access privileges may be terminated, appropriate disciplinary action taken in accordance with the Student Code of Conduct, and all future access could be denied.

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 Internet usage 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. 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.
3. 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 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 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) 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 Coordinator Responsibilities

The technology coordinator 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 software loaded on computers in the District is consistent with District standards and is properly licensed.
3. 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.
4. Set limits for data storage within the District's system, as needed.

Principal Responsibilities

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

1. Ensure that all student users of network services annually complete a **SNRC**. All such agreements will be maintained in the principal's office, with copies sent to the technology coordinator.
2. Be responsible for disseminating and enforcing **SNRC** for the District's network Services, as well as any additional network rules as needed.
3. Ensure that campus employees 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 employees supervising students who use network services provide training emphasizing the appropriate use of this resource.
5. Campus principals must notify the technology coordinator or technologist, and all campus teachers by e-mail to cancel system privileges of students.

Individual User Responsibilities

The following standards will apply to all student 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. 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 technologist.
3. Accessing e-mail from other than a District provided e-mail account from any district computer is at all times prohibited without written permission from the Technology Director.
4. 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.
5. Students may not use the network computers when supervised by a substitute teacher.
6. When any classroom computer is logged in, the system user must be present, or the door or workstation locked.
7. 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.
8. Students may not disable, attempt to disable, bypass or attempt to bypass a filtering device on any network services computer.
9. Communications or other data may not be encrypted so as to avoid security review by system administrators.
10. System users may not use another person's system account without written permission from the technology coordinator or technologist. Teachers may, however, log on to any student account as needed.
11. Students may not reveal their system password to anyone other than a supervising teacher. Students must provide their system password to any supervisor when requested.

12. 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.
13. 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.
14. Students 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.
15. 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.
16. Students may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
17. Students may not access internet resources that use audio or video streaming without prior permission from the supervising teacher.
18. Students may not gain or attempt to gain unauthorized access to resources or information.
19. Students are forbidden from installing any programs or copyrighted material on any computer connected to PGISD network services. Only the technology coordinator, technologist or technology assistant may install programs or copyrighted material.
20. Playing games accessed through the internet is prohibited.
21. District computers that are used off campus may not be connected to the network. District computers being used off campus may not be connected to the internet.
22. 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.

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.

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

Students and parents 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 student knowingly bringing prohibited materials into the school's electronic environment may be subject to suspension of access and/or revocation of privileges on the District's system and may be subject to disciplinary action in accordance with

the Student Code of Conduct. 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.

Intellectual Property Rights
Students shall retain all rights to work they create using the District's electronic communication system.

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 coordinator.

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.

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.

Termination/Revocation of Network Services Access

Termination of an employee's or a student's access for violation of District policies or regulations 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

Student Network Responsibility Contract

I understand and will abide by the terms and conditions as outlined in the **Student Network Responsibility Contract** for use of PGISD network services. Should I commit any violation, my access privileges may be revoked, school disciplinary action according to the student Code of Conduct may be taken and/or appropriate legal action pursued.

Student Name: (please print)_____

Current Grade Level: ____

Student Signature: _____Date_____

_____

Parent or Guardian Network Responsibility Contract

As the parent or guardian of the above student, I have read the terms and conditions as outlined in the **Student Network Responsibility Contract** for use of PGISD network services. I understand that these privileges are designed for educational purposes.

In consideration for the privilege of using PGISD 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 my child's use of, or inability to use, the system, including, without limitations, the type of damage identified in the **Student Network Responsibility Contract**.

_____ I hereby give permission for my child to utilize PGISD network services.

_____ I do not give permission for my child to utilize PGISD network services.

Parent or Guardian Name (please print): _____

Parent or Guardian Signature: _____Date_____