PEASTER ISD COMPUTER NETWORK
ACCEPTABLE USE AGREEMENT

INTRODUCTION

The Superintendent or designee will oversee the District's computer network system.

The primary purpose for the District's computer network is for administrative and educational purposes consistent with the District's mission and goals. To remain eligible as a network user, the use of an account must be in support of and consistent with the educational objectives of the District. Therefore, all users of the Peaster Independent School District system must read and agree in writing to comply with the rules and guidelines incorporated into this document.

System users and parents of students with access to the District's computer network should be aware that users will be provided access via the Internet to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material. While the District will take reasonable steps to restrict access to such material, it is not possible to absolutely prevent such access. In addition, the smooth operation of the network relies upon the proper conduct of end users who must adhere to guidelines. These guidelines are provided so that users are aware of the responsibilities they are about to acquire.

COPYRIGHT & LICENSING COMPLIANCE

Most software is copyrighted and licensed and can only be used with the permission of the copyright holder. Therefore, no software may be installed on any device maintained by the District without authorization from the District's technology director. Additionally, no District-owned software may be copied or installed on any non-District devices except where licensing agreements allow for dual use.

All users are required to adhere to the District policy concerning Fair Use Guidelines as they relate to any form of intellectual property including but not limited to: text, visual, audio, and software materials. Users should assume that all materials available on the Internet are protected by copyright. Downloading or streaming unauthorized copies of copyrighted movies and music (even via shared folders or Google Drive) is prohibited.

No original work created by any student will be posted on a web page under the District's control unless the District has received consent from the student who created the work.

DISTRICT WEB PAGES AND RELEASE OF STUDENT INFORMATION

The District has established an Internet web site that presents information about the District. The webmaster will be responsible for maintaining the District website. Designated District personnel may be permitted to post information directly to the District web site and will therefore be held responsible for its content. Content on the website should be updated regularly and adhere to current standards.

Recognizing the Internet as an effective tool for communicating important news, classroom activities, extracurricular events, etc., the District reserves the right to publish relevant student information (including name, individual images, images as part of a group, videotaped images, voice recordings, and extracurricular memberships) to the District's web site. Parents may restrict the publishing of their child's information (in whole or in part) by sending written notice to their child's campus principal.

All District web pages shall be subject to approval or modification by the technology director for purposes of protecting individual privacy and adherence to District policy on release of information and copyright.

THIRD PARTY ACCOUNTS

In accordance with our District mission, goals and vision our students may require accounts in third-party systems. Many of these accounts will be used at school for school related projects but may also be accessed outside of school with their parents' permission. The use of these accounts will help our students to master effective and proper online communications as required in the PreK-12 Technology Applications Standards. The District reserves the right to create and manage third party accounts (including but not limited to: Destiny, Discovery Education, Study Island, Learning.com, HMH, Pearson, Edgenuity, Apple, Google, Microsoft Office 365, Adobe) for students. Parents may deny the District permission to create and manage third-party accounts by sending written notice to their child's campus principal.

COMPUTER AND NETWORK ACCESS

Access to the District's computer network system will be governed as follows:

1. No one will be granted access to the District's secure network without agreeing beforehand to abide by this Acceptable Use Agreement.
2. Members of the public shall be allowed access to the District's public wireless network in designated locations if such use does not impose a tangible cost to the District and does not unduly burden the District's computer or network resources. Such access will be filtered by the District's Internet content filter.
3. Access to the District computer network and the Internet is a privilege, not a right. Inappropriate use will have consequences. The District may suspend or revoke a user's access if identified as a security risk or upon violation of the District's acceptable use agreement or device use agreement.
4. Monitoring of student Internet and device use is the responsibility of all District staff.
5. Students completing coursework will have first priority for use of District resources.
6. Students will have their accounts disabled effective on or after their withdrawal date.
7. Employees will have their accounts disabled upon the completion of their employment duties as specified by human resources.

INTERNET SAFETY

In an effort to provide a safe online environment for students while on the Internet, the District shall:

1. Implement an Internet content filter to block access to sites that contain content that is obscene, pornographic, or harmful to minors. The District may also limit access to sites based on additional factors such as network security, viruses/malware and Internet bandwidth limitations.
2. Authorize the technology director to override the content filter during use by an adult to allow access for bona fide research or other lawful purposes.
3. Prevent unauthorized access, including hacking and other unlawful activities by requiring the use of security credentials to access the secure system, firewalls, and other commonly acceptable security measures.
4. Restrict the unauthorized disclosure, use, and dissemination of personally identifiable student information.
5. Educate minors and staff about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms, and cyberbullying awareness.

TECHNOLOGY DIRECTOR RESPONSIBILITIES

The technology director for the District's computer will:

1. Be responsible for disseminating and enforcing applicable District policies and the acceptable use agreement for the District's system.
2. Ensure that all users of the District's secure network complete an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on

file and accessible for review by appropriate District personnel.
3. Ensure that employees who use the District's system are provided training emphasizing the appropriate, ethical, and safe use of this resource.
4. Ensure that District software is compatible with current standards and is properly licensed.
5. Be authorized to monitor or examine all system activities (both local and third-party, i.e. Google Workspace for Education) including electronic mail transmissions, electronic message postings, and all electronic data stored within the system and delete any files as deemed necessary to ensure proper and appropriate use of the system. This includes all activity on school owned devices whether used on or off the school network.
6. Set limits for data and email storage within the District's system, as needed.
7. Deny, revoke, or suspend specific user accounts, with or without cause or notice, for violations of acceptable use policies, or as a result of other disciplinary actions against the user.

PERSONAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's computer network system:

General Guidelines

1. Users shall not use the system for unlawful purposes, commercial activities, financial gain, or fraud.
2. Users shall not take or post photos, videos or audio recordings of others without their prior permission.
3. No user activity or data on District issued systems should be considered private by any user.
4. Data stored on District issued systems by students may be deleted at the conclusion of each school year. Students should make a backup on removable media of any data they want to preserve.
5. Data stored on District issued systems by employees will generally be accessible the following school year. However, employees should backup all data they want to preserve both periodically as well as at the conclusion of each school year.

Online Use

1. The individual for whom an account is issued will be responsible at all times for its proper use.
2. Users may not use another person's account, attempt to discover another user's password, nor reveal their own password to anyone.
3. Users may not attempt to gain unauthorized access to restricted systems, websites, or resources.
4. Users shall not access, create, store, or transmit information or materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
5. Visits to objectionable sites on the Internet or accessing any other inappropriate material may result in suspension or revocation of system privileges. Any user who gains access to inappropriate material is expected to discontinue the access as quickly as possible and report the incident to their teacher, supervisor, or the technology director.
6. Users shall not deliberately annoy or harass others using a District device, network, or account.
7. Users shall not intentionally erase, rename, modify, or damage data belonging to others.
8. Reproducing another student's work (in part or in whole) for purposes of academic cheating is classified as plagiarism/forgery and may result in the suspension or revocation of system privileges as well as other consequences consistent with the Student Code of Conduct.
9. Users shall use the Peaster ISD computer network resources primarily for instructional or administrative purposes. Users shall be permitted limited personal use as appropriate if such use does not impose a tangible cost to the District, does not unduly burden the District's computer or network resources, does not adversely affect the student's academic performance or employee's job performance, and does not violate any other element of the Acceptable Use Agreement.

Hardware & Software Use

1. Use of non-District owned devices on the District's guest network is allowed.
2. Users shall not utilize a hotspot device or enable the hotspot feature of a personal mobile device at school. Such devices can interfere with the District's network and bypass Internet safety systems.
3. Users shall not install, tamper with or relocate fixed computers, printers, phones, access points or other associated system equipment without authorization from the technology department.
4. Vandalism or damage to equipment arising from excessively irresponsible behavior will require restitution for costs associated with system restoration, hardware, or software costs as well as other appropriate consequences.
5. Software may not be installed on any device maintained by the District (other than those from the Apple App Store or Chrome web store) without authorization from the District's technology director. Additionally, no District-owned software may be copied or installed on any non-District devices except where licensing agreements allow for dual use privileges.
6. Users may not delete or modify system-wide files or settings.
7. Users shall not write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Deliberate attempts to degrade or disrupt system performance are violations of District policy and may constitute criminal activity under applicable state and federal laws.

Electronic Communications

1. Electronic mail (e-mail) is not private. Technology administrators have access to email and messages may be subject to Open Records Act requests (whether sent using District email or third party email). Messages relating to or in support of illegal activities will be reported to the authorities.
2. Access to District electronic mail shall be password protected if stored on a personal electronic device (such as smartphone, tablet, etc.)
3. System users should be mindful that use of school-related electronic 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.
4. Sending or attempting to send mass electronic mail messages as advertising for purchase or sale of non-school related products is prohibited.
5. Sending or attempting to send electronic mail messages for personal political use to advocate for or against a candidate, officeholder, or political party is prohibited.
6. Sending or attempting to send electronic mail messages as another user is prohibited. Unauthorized attempts to read, delete, copy, or modify the electronic mail of other users or deliberate interference with the ability of other users to send/receive electronic mail is prohibited.
7. Students are prohibited from participating in any email, chat room, newsgroup, bulletin board, or instant messaging system accessed on the Internet during the school day, except that which may be expressly provided by the District (such as Google Workspace for Education, etc.).
8. Employees are prohibited from participating in any chat room, newsgroup, bulletin board, or instant messaging system accessed on the Internet during the school day, except that which may be expressly provided by the District (such as Google Workspace for Education, etc.) or as appropriate to their employment function and in accordance with District policies.
9. District employees are expected to appropriately maintain any email or voicemail account that may be issued to them.
10. Employees should become familiar with and adhere to the District's policy regarding personal use of electronic media (Policy DH Local), communications with students via electronic media (Policy DH Local), and obligations to retain electronic records (Policy CQ Local). Refer to the employee handbook for guidance in these areas.

Network Etiquette and Privacy
Users are expected to abide by the generally accepted rules of network and Internet etiquette. These rules include (but are not limited to) the following:

- BE POLITE: Never send or encourage others to send abusive messages or posts. Never take or post photos, videos or audio recordings of others without their prior permission.
- BE APPROPRIATE: Remember that you are a representative of our school and District. Swearing, vulgarity, ethnic or racial slurs, sexual innuendos, and any other inflammatory language is prohibited. Transmitting or receiving obscene messages or pictures is prohibited.
- BE HONEST: Pretending to be someone else when sending/receiving messages is prohibited. Respect the copyright of others' words, images, etc.
- BE SAFE: Do not distribute personal information about yourself or others online. Additionally, students should not agree to meet someone they met on-line without parental knowledge or participation.
- DISRUPTIONS: Using the network in such a way that will disrupt the use of the network by other users is prohibited. Additionally, users should not engage in digital activities that will disrupt the learning environment of others.

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 or 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 system.

Peaster Independent School District will not be responsible for any damages suffered while on this system. These damages include loss of data as a result of delays, non-deliveries, misdeliveries, or service interruptions caused by the system or user errors or omissions. Use of any information obtained via the system is at your own risk. Peaster Independent School District specifically disclaims any responsibility for the accuracy of information obtained through its services.