EMPLOYEE AGREEMENT FORM FOR ACCEPTABLE USE OF PEASTER ISD COMPUTER NETWORK

The opportunity to use the District's computer network comes with responsibility. Inappropriate system use may result in the loss of the privilege to use this educational tool. Therefore, it is important that you read the complete version of the Peaster ISD Computer Network Acceptable Use Agreement (available online at https://peasternet.finalsite.com/fs/admin/site/pages/639), the employee agreement form, and ask questions if unclear. This page simply provides a partial summary of the full document.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may encounter some material you might find objectionable. While the District will take reasonable steps to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

RULES FOR APPROPRIATE USE

- You may be assigned an individual account for your use only. You are responsible for not sharing the password for your account with anyone (students, children, colleagues, etc).
- The account is to be used mainly for identified educational purposes, but some limited personal use is permitted as long as it 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 employee's job performance nor disrupt the learning environment, and does not violate any other element of the AUP.
- Neither your computer use nor email is private. Activity may be monitored and messages may be subject to Open Records Act requests. Any illegal activity will be reported to the appropriate agencies.
- Remember that people who receive e-mail from you with a school address might think your message represents the school's point of view.
- Access to District electronic mail shall be password protected if stored on a personal electronic device.
- Employees should become familiar with and adhere to the District's policy regarding personal use of electronic media (Policy DH Local) and obligations to retain electronic records (Policy CQ Local).
- You will be held responsible at all times for the proper use of your accounts. The District may suspend or revoke your access if you violate the rules.
- Notify a supervisor or the Director of Technology immediately if inappropriate content is accessed.
- You must take precautions to protect against cybersecurity threats including ransomware and unauthorized release of personally identifiable information of students. Annual cybersecurity training will be required.

INAPPROPRIATE USES

- Using the system for any unlawful purposes, commercial activities, financial gain, or fraud.
- Using someone else's network or email account with or without their permission.
- Downloading or streaming unauthorized copyrighted movies/music via shared folders or Google Drive.
- Downloading or using copyrighted information without permission from the copyright holder.
- Taking or posting photos, videos or audio recordings of others without their prior permission.
- Downloading or installing software (other than those from the Apple App Store or Chrome web store) on the District system without authorization from the technology director.
- Sending mass electronic mail messages as advertising for purchase or sale of products.
- 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.
- Posting messages, sending emails, or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Wasting school resources through the improper use of the computer system.
- Attempting to modify or damage the computer network or devices related to it.
- Gaining or attempting to gain unauthorized access to restricted websites, information, or resources.
- Accessing any instant messaging or chat system except that which may be provided by the District.
- Connecting a non-District owned device to a secure District network without prior authorization. Non-District devices may use the Guest networks available at all campuses.

CONSEQUENCES FOR INAPPROPRIATE USES

- Suspension of access to the system.
- Revocation of the computer system account.
- Other disciplinary or legal action in accordance with the District policies and applicable laws.
- Restitution for costs associated with system restoration, hardware, or software costs.