GOOSE CREEK CONSOLIDATED INDEPENDENT SCHOOL DISTRICT

June 2024

Attachment C

Contractor Access for Login & Email

Contractor Information

Print Name:_____ Job Title:_____

Print Name as it appears on your social Security Card

Location:_____

Start Date:_____ End Date:_____

The computer network at Goose Creek CISD is vital to the daily operations of our district. Managing ethical computer behavior is of the utmost importance. Computer ethics are guidelines that govern the use of computers, networks, and information systems. It deals with how technology professionals make decisions regarding professional and social conduct. GCCISD must control computer and network security risks. A computer or network security risk is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability. This includes unauthorized access and use; software theft, information theft, viruses, hacking, tampering with system files, or remotely accessing another's computer without their knowing. Responsibilities outlined as follows:

- Uphold any and all information privacy of all users and students. Information privacy includes electronic profiles, cookies, spyware, and user/employee monitoring. Do not use any computer to observe, record, or review a user or employee's computer use. Do not steal information, including anything personal or confidential. Never access a computer, its data, or the network for unapproved or illegal activities.
- Safeguard against hardware theft and vandalism. Hardware theft is the act of stealing computer equipment. Hardware vandalism is the act of defacing or destroying computer equipment.
- Protect software manufacturers against software piracy. Software piracy is the unauthorized and illegal duplication of copyrighted software. Abide by the software manufacturers license agreement that provides specific conditions for use of the software.
- Safeguard against computer viruses, worms, and trojan horses. This includes any potentially damaging or damaging program that affects, or infects, a computer negatively by altering the way the computer works. Always take precautions to guard against these malicious-logic programs. For example, do not start a computer with an external source. Never open an e-mail attachment unless it is from a trusted source. Disable macros in documents that are not from a trusted source. Stay informed about any new virus alert or virus hoax.
- Be responsible for managing all computer and network security risks. A computer or network security risk is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability. This includes unauthorized access and use; software theft, information theft, viruses, hacking, tampering with system files, or remotely accessing another's computer without their knowing.
- Network rights and Internet access granted to contractors are solely for the purpose of accessing network resources to fulfill the task assigned, and only that task.
- Account will be active until the last day of the school year. A new form must be filled out each school year for security access

Describe Access Needed:	Justification:

By signing below, you are acknowledging that you have read the district's Security Policy for Personal Computing and Electronic Communications and agree to abide by the stated provisions and by following the Acceptable Use Guidelines located here:
https://schools.gccisd.net/upload/page/1173/GCCISD%20Acceptable%20Use%20Guidelines%206-27-24.pdf
In consideration for the privilege of using the district's electronic communications system, 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 use of, or inability to use, the system, including, without limitation, the type of damages identified in the district's policy and administrative regulations. I also understand the responsibilities of authorized users and understand that intentional misuse of data and/or computers can result in legal action.

Users Signature:_____ **Date:**_____

Print Name of Director, Principal or Supervisor:_____

Signature of Director, Principal or Supervisor:_____