Gonzales Independent School District

Technology Policies and Procedures/ Acceptable Use Manual

John Schumacher – Superintendent

Jenny Needham – Director of Technology

John Owens – District Systems Integrator

Rutty Decou – District Network Technician

Instructional Technologist –

Julie Burek - District Support (Accounts/Training)

Abbie Dolezal – District Technologist

Elizabeth Alvarez – Administrative Assistant

www.gonzalesisd.net

Gonzales ISD Acceptable Use Policy for Technology

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

1. Imposes no tangible costs to the District;
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

Students and employees will be provided training in the use of the District's Electronic Communication and Data Management System prior to being issued a user account. All training in the use of the District's system will emphasize ethical use of this resource.

System Access

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
3. System users may not disable, or attempt to disable or bypass the Internet filtering while at school in any way, including using a modem, telephone connection, or VPN.
4. System users may not encrypt communications so as to avoid security review by the system administrator.
5. System users may not use another person's system account.
6. System users must avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages from unknown senders or that are suspicious in subject or content that ask you to follow a link and bringing disks, USB, and external "flash drive" devices used on other systems.
7. Users are not allowed to change settings on any computer or load software onto any district computer system without prior authorization by the Director of Technology.
8. System users may not send or post messages to message boards that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
9. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
10. System users may not waste District resources related to the system.
11. System users may not gain unauthorized access to resources or information.
12. The use of social media, *not approved by administration*, such as Facebook and Twitter, for classroom/instructional use is disallowed.

System User Account Disclaimer

The District's system is 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, advise, 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.

Network Etiquette
System users are expected to observe the following network etiquette:
1. Be polite. Messages typed in capital letters are the computer equivalent of shouting and are considered to be rude.
2. Use appropriate language. Swearing, vulgarity, ethnic and racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is prohibited.
4. Transmitting obscene messages or pictures is prohibited.
5. E-mail attachments must be of a reasonable size and in a format readable by the receiver.
6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

Termination/Revocation of System User Account
The District may suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.

Vandalism
Any malicious attempt to harm or destroy District equipment or data, or the data of another user of the District's system, or 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, uploading or creating of computer viruses.

Forgery
Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's ID and/or password is prohibited.

System users are advised that despite the District's use of filtering and monitoring, these measures may not prevent access to other electronic communications systems in the global electronic community that could contain inaccurate and/or objectionable material.

An employee who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to their supervisor and the Technology Department. An employee knowingly bringing prohibited materials into the District's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subjected to disciplinary action in accordance with the District's policies.

Assigned Equipment
The equipment you have been issued is your responsibility. *This equipment is not to be moved or reassigned without the permission of the Director of Technology.* Each device has been inventoried and its location noted. It will be checked at the beginning and end of each year.

Device Security
1. Log off or Lock workstation (CTRL-ALT-DEL or Windows + L) if you are away from your computer.
2. Maintain a secure password for all devices issued by GISD.
3. System users should never share their password with anyone. If another system user needs access to your device, have them log on with their own credentials.
4. Do not leave devices unattended. This causes an increased chance of theft or security breach.
5. Do not use thumb prints as security passwords for login.

Teacher Laptop
1. You may install Internet Service Provider software, home printer software, and camera software without additional consent. Submit a work order if an administrative password is required.
2. Other software applications must be approved in writing. (Rule of Thumb – anything that has to be installed must be cleared by the Director of Technology). Installing software increases your risk of malware.

E-Mail
System users are expected to observe the following e-mail rules:
1. System users are prohibited from using unauthorized e-mail services.
2. System users will only be able to use e-mail accounts issued by GISD for all communication with GISD staff, students and parents/guardians.
3. All e-mail accounts may be monitored by system administrator.
4. Use e-mail in such a way that will not disrupt the use of the network.
5. Mass emails by anyone other than administration are not allowed.
6. Solicitation is prohibited.
7. Anything sent in an email should be archived.
8. Anything sent in an email is subject to open records policies.

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 Director of Public Relations (PR). Staff accounts for website content are created by the Technology Department.

All campuses must maintain their website with the most recent information available. All information posted on GISD campus pages must be checked for accuracy and compliance. Please check the student's permission status on the Release of Directory Information form, Sections 3&4, before publishing any student's photo or information.

Facebook
The Director of Public Relations will maintain administrative rights to a district level Facebook page. All Other Facebook pages must be approved by the Director of Public Relations (PR) and a link provided giving GISD PR administrative rights to that page. A link to that page will be put on the district website and app. All information posted on GISD Facebook pages must be checked for accuracy and compliance. Please check the student's permission status on the Release of Directory Information form, Sections 3&4, before publishing any student's photo or information.

Blackboard Mass Media Notifications
The Administrative Office will be responsible for broadcasting any emergency information involving the entire district. It will use all modalities available, including Blackboard call out, email, app, and text, the district website, radio, TV, etc.

The campuses have the Blackboard system at their disposal. Please keep in mind that mass phone call should be reserved for the most vital information. Blackboard allows campuses to send email, text messages, and messages through the app. These should be used for regular, every day communication with the parents/guardians of the students. Be cognizant of the number of messages and times they are sent.

Participation in Online Programs/Applications
Students are prohibited from participating in any instant messaging, social media accessed on the Internet unless it is a secure program set up by their teacher for their class. Such participation is permissible for employees as a resource to perform their jobs.

Classroom Phone
Each classroom will have a phone with voicemail, assigned to the respective teacher.

Personal Devices on Our System
1. Personal devices are allowed on our GISD Student/Guest network, where available, as long as it is not interfering with the educational use of our bandwidth.

Troubleshooting Technology Issues
1. There are helpful instructions and videos on the website.
www.gonzalesisd.net > Departments > Technology
2. If you are unable to solve your issue, submit a work order. Please do not contact directly District Technology Staff by cell phone, email, or any other means to resolve an issue.

Gonzales Independent School District
Agreement for Responsible Use of Electronic Communication System

I understand that my computer use is not private and that the District may monitor activity to include but not limited to any online communication, home directories, and electronic resources, on any GISD computer system to which I may have access.

I have read the District's electronic communication system rules and agree to abide by these provisions. In consideration for the privilege of using the District's electronic communications system and in consideration for having access to the Internet, 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 administration regulations.

Employee Name (Printed) _____

Location _____

Employee Signature _____ Date _____