GAINESVILLE INDEPENDENT SCHOOL DISTRICT
EMPLOYEES GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES

These guidelines are provided here so that employees are aware of the responsibilities they accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs/DVDs, digitized information, communication technologies, and Internet access. In general, this requires efficient, ethical, and legal use of all technology resources.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some material you find objectionable. While the District will use filtering technology 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.

1. Expectations

a. Use of computers, other technical hardware, computer networks, and software is only allowed when granted permission by the employee's supervisor.

b. All users are expected to follow existing copyright laws. United State Copyright Law, 17 U.S.C. 101-1332 governs the use of copyrighted materials. However, technology has outpaced the law and limits of what we can do with copyrighted material.

c. Employees are expected to notify their supervisor or the technology director whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

d. Employees who identify or know about a security problem are expected to convey the details to their supervisor or the technology director without discussing it with others.

e. Employees are responsible for securing technology devices when not in use and for returning them in good working condition.

DISCLAIMER OF LIABILITY: The district shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, in appropriate use of third party sites or costs incurred by a user. The district shall not be responsible for ensuring the accuracy or usability of any information found on the Internet. 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 users' requirements or the system will be uninterrupted or error-free. The District shall not be liable for lost, stolen, or damaged devices brought from home.

2. Unacceptable Conduct (includes the following, but is not limited to)

a. Using the network for illegal activities, including copyright or contract violations, or downloading inappropriate materials, viruses, and/or software, such as but not limited to hacking and host file sharing software.

b. Using the network for financial or commercial gain, advertising, or political lobbying.

c. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites, social networking sites (i.e. Facebook, Twitter, Snapchat, Instagram, etc.), as well as chat and/or blog sites.

(1) Social Media Guidelines (see also *Personal Use of Electronic Media*):

According to the Texas Education Agency Educators' Code of Ethics, educators *must refrain from inappropriately communicating with students through the use of social media.*

(I) Standard 3.9. The educator shall refrain from inappropriate communication with a student or minor, including, but not limited to, electronic communication such as cell phone, text messaging, e-mail, instant messaging, blogging, or other social network communication. Factors that may be considered in assessing whether the communication is inappropriate include, but are not limited to:

(i) the nature, purpose, timing, and amount of the communication; (ii) the subject matter of the communication; (iii) whether the communication was made openly or the educator attempted to conceal the communication; (iv) whether the communication could be reasonably interpreted as soliciting sexual contact or a romantic relationship; (v) whether the communication was sexually explicit; and (vi) whether the communication involved discussion(s) of the physical or sexual attractiveness or the sexual history, activities, preferences, or fantasies of either the educator or the student.

d. Vandalizing and/or tampering with equipment, programs, files, software, system performance or other components of the network. Use or possession of hacking software is strictly prohibited.

e. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals. Intentionally wasting finite resources (i.e., online time, real-time music and/or video not for educational purpose).

f. Gaining unauthorized access anywhere on the network.

g. Disabling or attempting to disable any Internet filtering device.

h. Revealing identifying information such as the home address or phone number of one's self or another person.

i. Invading the privacy of other individuals.

j. Using another user's account, password, or ID card or allowing another user access to your account, password, or ID.

k. Coaching, helping, observing, or joining any unauthorized activity on the network.

l. Forwarding/distributing e-mail messages without permission from the author.

m. Posting anonymous messages or unlawful information on the system.

n. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, demeaning, slanderous.

o. Falsifying permission, authorization of identification documents.

p. Violating copyrighted information or others' intellectual property rights as well as downloading or using copyrighted information without permission from the copyright holder.

q. Obtain copies of or modify files, data, or passwords belonging to other users on the network.

r. Knowingly placing a computer virus on a computer or network.

s. Allow a student on a teacher computer.

3. Acceptable Use Guidelines

a. General Guidelines

(1) All employees will have access to all available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.

(2) Employees are responsible for their ethical and educational use of the computer online services in the District.

(3) All policies and restrictions of the GISD computer online services must be followed.

(4) Access to the District's GISD computer online services is a privilege and not a right. Each employee will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Policy Agreement Sheet in order to be granted access to GISD computer online services.

(5) The use of any GISD computer online services in the District must be in support of education and research and in support of the educational goals and objectives of the District.

(6) Transmission of any material that is in violation of any federal or state law is prohibited. This includes but is not limited to: student or other confidential information, copyrighted material, threatening or obscene material, and computer viruses.

(7) Employees must comply with Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student and District records.

(8) Any attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the individual campus administrator or technology administrator will be considered an act of vandalism and subject to disciplinary action in accordance with Board policy.

b. Network Etiquette

(1) Be polite.

(2) Use appropriate language.

(3) Do not reveal personal data (home address, phone number, or phone numbers of other people).

(4) Remember that the other users of the GISD computer online services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

c. E-Mail

(1) E-mail should be used for educational or administrative purposes only.

(2) All e-mail and all contents are property of the District.

(3) All e-mail is archived for a minimum of three (3) years.

(4) E-mail transmissions, stored data, transmitted data, or any other use of the GISD computer online services by employees or any other user will not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

d. Personal Use of Electronic Media

Electronic media includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), electronic forums (chat rooms), video sharing Web sites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, Twitter, Snapchat, Instagram, LinkedIn). Electronic media also includes all forms of telecommunication such as landlines, cell phones, and Web-based applications.

As role models for the district's students, employees are responsible for their public conduct even when they are not acting as district employees. Employees will be held to the same professional standards in their public use of electronic media as they are for any other public conduct. If an employee's use of electronic media interferes with the employee's ability of effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment. If an employee wishes to use a social network site or similar media for personal purposes, the employee is responsible for the content on the employee's page, including content added by the employee, the employee's friends, or members of the public who can access the employee's page, and for Web links on the employee's page. The employee is also responsible for maintaining privacy settings appropriate to the content.

An employee who uses electronic media for personal purposes shall observe the following:

- The employee may not setup or update the employee's personal social network page(s) using the district's computers, network or equipment.
- The employee shall not use the district's logo or other copyrighted material of the district without express written consent.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off campus. These restrictions include:
    - Confidentiality of student records.
    - Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law.
    - Confidentiality of district records, including educator evaluations and private e-mail addresses.
    - Copyright law
    - Prohibition against harming others by knowingly making false statement about a colleague or the school system.

f. Personal Use of Electronic Media with Students

A certified or licensed employee, or any other employee designated in writing by the superintendent or a campus principal, may communicate through electronic media with students who are currently enrolled in the district. the employee must comply with the provisions outlined below. All other employees are prohibited from communicating with students who are enrolled in the district through electronic media.

An employee is not subject to these provisions to the extent the employee has a social or family relationship with the student. For example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational or religious organization.

The following definitions apply for the use of electronic media with students:

- *Electronic media* includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), electronic forums (chat rooms), video sharing Web sites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, Twitter, Snapchat, Instagram, LinkedIn). Electronic media also includes all forms of telecommunication such as landlines, cell phones, and Web-based applications.

- *Communicate* means to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee's personal social network page or a blog) is not a *communication*: however, the employee may be subject to district regulations on personal electronic communications. Unsolicited contact from a student through electronic means is not a *communication*.

- *Certified or licensed employee* means a person employed in a position requiring SBEC certification or a professional license, and whose job duties may require the employee to communicate electronically with students. The term includes classroom teachers, counselors, principals, librarians, paraprofessionals, nurses, educational diagnosticians, licensed therapists, and athletic trainers.

An employee who uses electronic media for personal purposes shall observe the following:

- The employee is prohibited from knowingly communicating with students using any form of electronic communications, including mobile and Web applications, that are not provided or accessible by the district unless specific exception is noted below.

- Only a teacher, trainer, or other employee who has an extracurricular duty may use text messaging, and then only to communicate with student who participate in the extracurricular activity over which the employee has responsibility. An employee who communicates with a student using text messaging shall comply with the following protocol:
  - For each text message addressed to one or more students, the employee shall send a copy of the text message to the employee's district e-mail address.
  - The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity).
  - The employee is prohibited from knowingly communicating with students through a personal social network page; the employee must create a separate social network page ("professional page") for the purpose of communicating with students. The employee must enable administration and parents to access the employee's professional page.
  - The employee shall not communicate directly with any student between the hours of 9:00 p.m. and 6:00 a.m. An employee may, however, make public posts to a social network site, blog, or similar application at any time.

- The employee does not have a right to privacy with respect to communications with students and parents.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators including:
    - Compliance with the Public Information Act and Family Educational Right and Privacy Act (FERPA), including retention and confidentiality of student records.
    - Copyright law
    - Prohibitions against soliciting and engaging in sexual conduct or a romantic relationship with a student.
- Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with any one or more currently-enrolled students.
- Upon written request from a parent or student, the employee shall discontinue communicating with the student through e-mail, text messaging, instant messaging, or any other form of one-to-one communication.

An employee may request an exception form one or more of the limitations above by submitting a written request to his or her immediate supervisor.

g. Consequences

The employee, in whose name a system account and/or computer hardware is issued, will be responsible at all times for its appropriate use.

Noncompliance with the guidelines published here may result in suspension or termination of technology privileges and disciplinary actions. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 will result in criminal prosecution, as well as disciplinary actions by the District.

The District cooperates fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications using District equipment and network access is governed by the Texas Open Records Act, therefore, when legally requested, proper authorities will be given access to their content.

Gainesville ISD Employee Acceptable Use Policy Agreement

Employee Name (print) _____

School/Location _____

I have read the Employee Acceptable Use Guidelines for Gainesville ISD. I agree to follow the rules contained in these guidelines. I further understand that electronic mail transmissions and other use of the electronic communications systems, including the Internet, are not private and may be monitored at any time by the District staff to ensure appropriate use, as defined by the Acceptable Use Guidelines. I understand that violations can result in disciplinary action such as denial of access privileges, change in employment status, appropriate legal action, and/or termination of employment.

Employee Signature _____ Date_____