RESPONSIBLE USE PROCEDURES FOR GPISD EMPLOYEES

TECHNOLOGY RESOURCES

The district's technology resources, including its network access to the Internet, are primarily for administrative and instructional purposes. Limited personal use is permitted if the use:

- Imposes no tangible cost to the district.
- Does not unduly burden the district's technology resources; and
- Has no adverse effect on job performance or on a student's academic performance.

Electronic mail transmissions and other use of technology resources are not confidential and can be monitored at any time to ensure appropriate use.

Employees who are authorized to use the system are required to abide by the provisions of the district's responsible use policy and administrative procedures. Failure to do so can result in suspension of access or termination of privileges and may lead to disciplinary action.

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

Personal Use of Electronic Media

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 to 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, for personal purposes, a social network site or other media intended to build relationships with other users, 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.

Employees may load personal apps or other media to GPISD-owned devices assigned to the staff member. This limited personal use of resources is permitted if it does not impose a tangible cost to the district, does not unduly burden the district's technology resources and has no adverse effect on job performance or on a student's academic performance. However, employees must additionally use discernment when loading materials and setting privacy and sync operations. Staff members must not post, share or display anything (text, images, videos, apps, online subscriptions to books or magazines, music or otherwise) that would disrupt education, violate local, state or federal guidelines or negatively impact the perception of the employee's ability to be effective in their employment capacity. Such violations may be addressed by the District and could lead to disciplinary action up to and including termination.

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

- The employee may not set up or update the employee's personal social network page(s) using District email addresses, 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. See GPISD Board Policy FL (Local)
    - Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law. See GPISD Board Policy DH (Exhibit)
    - Confidentiality of district records, including educator evaluations and private email address. See GPISD Board Policy GA (Local)
    - Copyright law. See GPISD Board Policy CY (Local)
    - Prohibition against harming others by knowingly making false statements about a colleague or the school system. See GPISD Board Policy DH (EXHIBIT)
- See *Use of Electronic Media with Students*, below, for regulation on employee communication with students through electronic media.
- Personally loaded applications may not be supported by District Technology.

Use of Electronic Media with Students
GPISD Board Policy DH (Local)

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 a 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, email, blogs, electronic forums (chat rooms), video sharing websites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, MySpace, Twitter, 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. See *Personal Use of Electronic Media*, above. Unsolicited contact from a student through electronic means is not a communication.
- Certified or licensed employee means a person employed in a position required 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, Instructional Media Specialists, paraprofessionals, nurses, educational diagnosticians, licensed therapists, and athletic trainers.

An employee who uses electronic media to communicate with students shall observe the following:

- The employee may use any form of electronic media except text messaging. Only a teacher, trainer, or other employee who has an extracurricular duty may use text messaging, and then only to communicate with students 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:
    - The employee shall include at least one of the student's parents or guardians as a recipient on each text message to the student so that the student and parent receive the same message;
    - The employee shall include his or her immediate supervisor as a recipient on each text message to the student so that the student and supervisor receive the same message; or
    - 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 11 pm and 6 am. 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 the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records. See GPISD Board Policy CPC (Local) and FL (Local)
    - Copyright law. See GPISD Board Policy CY (Local)
    - Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student. See GPISD Board Policy DF (Local)
- 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 email, text messaging, instant messaging, or any other form of one-to-one communication.

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

ADDITIONAL GUIDELINES

Consequences

Violation of GPISD's policies and procedures concerning the use of computers and networks will result in the same disciplinary actions that would result from similar violations in other areas of GPISD. Improper or unethical use may result in disciplinary actions and, if appropriate, the Texas Penal Code, Computers Crimes, Chapter 33, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software costs. The district will cooperate fully with local, state, or federal officials in any invitation concerning or relating to misuse of the District's computer systems and networks.

Illegal Activity

Transmission (that is, uploading or downloading) of any material in violation of any national, state or local regulation is prohibited. This includes, but is not limited to:

- Copyrighted material
- Abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, illegal material
- Material protected by trade secret
- Commercial activities such as conducting private business on the Internet or through District email accounts
- Transmission for advertisement or political use

Consent

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the copyright owner, or an individual the owner specifically authorizes, may upload or redistribute copyrighted material to the system.

No original work created by and District student or employee will be posted on a web page under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor.)

No personally identifiable information about a District student will be posted on a web page under the District's control unless the District has received written consent from the student's parent. The *Family Educational Rights and Privacy Act* and District policy may make an exception for "directory information" as allowed.

Security

Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the network, you are required to notify a system administrator or school personnel. Do not demonstrate the problem to other users. Do not use another individual's account.

Etiquette

Users are expected to abide by the generally accepted rules of communications etiquette. These include, but are not limited to, the following:

- Be polite. Do not send or post abusive messages.
- Use appropriate language. Do not swear, use vulgarities, sexually suggestive language, or any other inappropriate language.
- Exercise caution when using GPISD communications tools to email or post your opinions. Recipients or other readers may assume that your opinion represents the views of the District or school, whether or not that was your intention.
- Do not reveal your personal address or phone number or the address or phone number of students or colleagues.
- Check your email at least once a day. Reply to email from parents or other public members who have legitimate business requests within 24 hours whenever possible.
- Share your GPISD email address with interested parents and community members who request to communicate with you in this fashion.
- Do not send messages to an entire staff when only a small group of people actually needs to receive the message. In accordance with established procedures, using email for commercial enterprises is prohibited.
- Do not forward messages that have no educational or professional value (e.g., chain letters.)

Monitored Use

Installed apps, email transmissions and other use of the system by employees are not private and may be monitored, reviewed, audited, intercepted, accessed, or disclosed at any time by designated District staff to ensure appropriate use, ensure the safety and integrity of the system, diagnose problems, and investigate reports of illegal or impermissible activities.

Users should be aware that the District will comply with lawful orders of courts, such as subpoenas and search warrants. The District is also subject to the Texas Public Information Act which may require disclosure of information transmitted through its system, including electronic communications.

Email

The following guidelines will apply to all users of the District's electronic communications systems:

- Users will be issued only one district email account, using their legal name.
- Communications may not be encrypted so as to avoid security review by system administrators.
- Attachments to email messages should include only data files. At no time should program files (e.g. .exe files) be attached due to risk of licensing violations and transmission of viruses.
- Requests for personal information on students or staff members should not be honored via email. This relates particularly to any requests for student grades, discipline, attendance or related information. In addition, security information such as usernames or passwords should not be sent via email for any reason.
- Staff members who correspond with students or parents must use only GPISD email to receive or send email.

Responsible Network Use

The individual in whose name a system account is issued will be responsible at all times for its proper use and to abide by the generally accepted guidelines for responsible network use. System users ***may not***:

- Utilize the District network for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
- Disable, or attempt to disable, a filtering device on the District's electronic communications system.
- Establish peer-to-peer networking.
- Create unauthorized wireless networks, including wireless access points, wireless routers and open networks on personal devices.
- Use any software or proxy service to obscure the student's IP address or sites that the student visits.
- Use another person's system account without written permission from the campus administrator.
- Gain unauthorized access to resources or information.
- Place the District network and equipment at risk of viruses and other harmful codes by opening email messages from unknown senders, loading data from unprotected computers, etc.

Equipment Guidelines

- All technology equipment should be shut down each evening.
- District personnel are responsible for District equipment if taken off school property. Staff members must secure items that are left on campus overnight. Employees may be held responsible for equipment that is damaged, lost or stolen.
- If an employee's District-issued equipment becomes damaged, lost or stolen, it is the employee's responsibility to report the issue to campus administration within 24 hours.