

BROWNSBORO INDEPENDENT SCHOOL DISTRICT

Employee Agreement for the Acceptable Use of the District's Electronic Communications System

District employees will be given access to the District's Electronic Communications System. **The Electronic Communications System is defined as the District's network, servers, computer workstations, telephones, peripherals, applications, databases, library catalog, online resources, Internet access, email, online class activities and any other technology designated for use by the District for employees.**

With this educational opportunity comes responsibility. It is important that employees read this agreement form, and then ask any questions if you need help understanding them. **The Employee Agreement for the Acceptable Use of the District's Electronic Communications System will apply to personal laptops and the use of personal laptops brought to the workplace.** Inappropriate system use of the District's Electronic Communications System will result in the consequences below, including loss of the privilege to use this educational tool.

Please acknowledge receipt and understanding of this form by completing and returning the Notice of Acknowledgement and Agreement Form in the back of this handbook.

Please note that Internet access is part of the District's Electronic Communications System. The Internet is a network of many types of communication and information networks, which are used frequently in classroom assignments and include access to library materials and purchased online databases. Some material accessible via the Internet may contain content that is illegal, inaccurate, or potentially offensive to employee. It is possible for employees to access (accidentally or otherwise) these areas of content. While the District uses filtering technology and protection measures to restrict access to such material, it is not possible to absolutely prevent such access. It will be each employee's responsibility to follow the rules for appropriate and acceptable use.

SOME RULES FOR APPROPRIATE USE

- Employees must only open, view, modify, and delete their own computer files, unless they have specific permission from a supervisor to do otherwise.
- Internet use at school must be primarily related to school assignments and projects.
- Employees may be assigned individual accounts to District resources and must use only those accounts and passwords that they have been granted permission by the District to use. All account activity should be for educational purposes only.
- Employees are responsible at all times for their use of the District's Electronic Communications System and must assume personal responsibility to behave ethically and responsibly, even when technology provides them the freedom to do otherwise.

SOME EXAMPLES OF INAPPROPRIATE USES

- Using the District's Electronic Communications System for illegal purposes (e.g. gambling, pornography, computer hacking).
- Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering or other security measures.
- Sharing your username and password with others, borrowing someone else's username (i.e. staff or student), password or account access.
- Purposefully opening, viewing, using, or deleting files belonging to another system user without permission.
- Electronically posting personal information about yourself or others (i.e., addresses, phone numbers, pictures).
- Downloading or plagiarizing copyrighted information without permission from the copyright holder.
- Intentionally introducing a virus or other malicious programs onto the District's system.
- Electronically posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Wasting or abusing school resources through unauthorized system use (e.g. online gaming, Internet radio, downloading music, watching videos, participating in chat rooms, checking personal email, etc).
- Gaining unauthorized access to restricted information or network resources.

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, MySpace, Twitter, 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 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 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 set up 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 statements about a colleague or the school system.

USE OF ELECTRIC 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 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, 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, 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 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 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.
- 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 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.
- Copyright law
- Prohibitions against soliciting or 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 from one or more of the limitations above by submitting a written request to his or her immediate supervisor.

PERSONAL WIRELESS DEVICES (laptops, iPods, iPads, etc.)

Personal laptops will be provided filtered access to the Internet as well as access to any web-based applications (e.g., gradebook, curriculum management system, DiscoveryStreaming, eFiles) that would normally be accessible to employees from home. Laptops are valuable devices that can be damaged. **The District is not responsible for the loss or theft of a personal laptop, nor for damage, nor unauthorized access to the device nor the data that resides therein.** In addition:

- Employees must take full responsibility for setting up and maintaining their personal laptops, charging them, etc. The District will not provide technical support for these devices including Work Orders/repairs/software installations.
- When laptops are not in the employee’s possession, they must be secured by the employee.
- An employee’s use of his/her laptop in the workplace must be primarily for job-related instructional and administrative purposes and in accordance with administrative regulations.
- Employee selection of appropriate, tasteful screen savers and wallpaper is expected.
- All employees with personal wireless devices must use the District provided wireless which is filtered according to the Children’s Internet Protection Act (CIPA) requirements. Employees are not to use non-District wireless service providers while on District property (cell phones, handheld devices, etc).
- **Personal laptops are not to be connected to the wired network.** They are only authorized for connectivity on the District’s public wireless network called BISD WiFi, unless otherwise directed by district Technology personnel.
- If an employee uses a personal laptop in an inappropriate manner, he/she will be subject to consequences for inappropriate use as outlined in the Employee Handbook, and this employee agreement form.

CONSEQUENCES FOR INAPPROPRIATE USE

- Suspension of access to the District’s Electronic Communications System
- Revocation of the District’s Electronic Communications System account(s); and/or
- Other appropriate disciplinary or legal action in accordance with applicable laws.

NOTE: The employee agreement to abide by these guidelines must be renewed each academic year. Also, District Policies and Administrative Regulations are included as an addendum to all handbooks for your review.