AN EARLY COLLEGE DISTRICT
JIM HOGG COUNTY
INDEPENDENT SCHOOL DISTRICT

Acceptable Use Policy

1. Overview

Jim Hogg County ISD's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Jim Hogg County ISD's established culture of openness, trust and integrity. Jim Hogg County ISD is committed to its employees & students from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Jim Hogg County ISD. These systems are to be used for business purposes in serving the interests of the district in the course of normal operations.

Effective security is a team effort involving the participation and support of every Jim Hogg County ISD employee and student who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Jim Hogg County ISD. These rules are in place to protect the employee, student and Jim Hogg County ISD. Inappropriate use exposes Jim Hogg County ISD to risks including virus attacks, compromise of network systems and services, and legal issues. District-owned devices will use the District's network, if applicable, and filtering regardless of location or Internet service provider. Any attempt to bypass the filter is prohibited.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Jim Hogg County ISD business or interact with internal networks and business systems, whether owned or leased by Jim Hogg County ISD, the employee, or a student. All employees, students, contractors, consultants, temporary, and other workers at Jim Hogg County ISD and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Jim Hogg County ISD policies and standards, and local laws and regulation. This policy applies to employees, students, contractors, consultants, temporaries, and other workers at Jim Hogg County ISD, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Jim Hogg County ISD.

4. Policy

4.1 General Use and Ownership

4.1.1 Jim Hogg County ISD proprietary information stored on electronic and computing devices whether owned or leased by Jim Hogg County ISD, the employee, student or a third party, remains the sole property of Jim Hogg County ISD. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Jim Hogg County ISD proprietary information.

4.1.3 You may access, use or share Jim Hogg County ISD proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties and or student assignment.

4.1.4 Employees & Students are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees & students should be guided by departmental policies on personal use, and if there is any uncertainty, employees & students should consult their campus administrator or staff in charge.

4.1.5 For security and network maintenance purposes, authorized individuals within Jim Hogg County ISD may monitor equipment, systems and network traffic at any time.

4.1.6 Jim Hogg County ISD reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 All mobile and computing devices that connect to the internal network must comply with the Acceptable Use Policy.

4.2.1 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.2 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.3 Postings by employees or students from a Jim Hogg County ISD email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Jim Hogg County ISD, unless posting is in the course of business duties.

4.2.4 Employees & students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees & students may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee or student of Jim Hogg County ISD authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Jim Hogg County ISD -owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Jim Hogg County ISD.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Jim Hogg County ISD or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting Jim Hogg County ISD business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a Jim Hogg County ISD computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any Jim Hogg County ISD account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee or student is not an intended recipient or logging into a server or account that the employee or student is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to Jim Hogg County ISD is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the Jim Hogg County ISD network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, Jim Hogg County ISD employees to parties outside Jim Hogg County ISD.

4.3.2 Email and Communication Activities

When using Jim Hogg County ISD resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the Technology Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within Jim Hogg County ISD's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Jim Hogg County ISD or connected via Jim Hogg County ISD's network.

4.3.3 Blogging and Social Media

1. Blogging by employees or students, whether using Jim Hogg County ISD’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Jim Hogg County ISD’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Jim Hogg County ISD’s policy, is not detrimental to Jim Hogg County ISD’s best interests, and does not interfere with an employee's regular work duties. Blogging from Jim Hogg County ISD’s systems is also subject to monitoring.

2. Jim Hogg County ISD’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Jim Hogg County ISD confidential or proprietary

information, trade secrets or any other material covered by Jim Hogg County ISD's Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Jim Hogg County ISD and/or any of its employees/students. Employees & students are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Jim Hogg County ISD's Non-Discrimination and Anti-Harassment policy.

4. Employees & students may also not attribute personal statements, opinions or beliefs to Jim Hogg County ISD when engaged in blogging. If an employee or student is expressing his or her beliefs and/or opinions in blogs, the employee or student may not, expressly or implicitly, represent themselves as an employee, student or representative of Jim Hogg County ISD. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Jim Hogg County ISD's trademarks, logos and any other Jim Hogg County ISD intellectual property may also not be used in connection with any blogging activity.

5. Policy Compliance

5.1 Compliance Measurement

The Jim Hogg County ISD Technology Department will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Jim Hogg County ISD Technology Department in advance.

5.3 Non-Compliance

An employee or student found to have violated this policy may be subject to disciplinary action according to the employee/student code of conduct & up to and including termination of employment. 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. Termination of an employee's account or of a student's access will be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

6. Definitions and Terms

- **Blogging:** To write about (an event, situation, topic, etc.) in a blog
- **Honeypot:** A honeypot is a decoy computer system for trapping hackers or tracking unconventional or new hacking methods. Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet.

- **Honeynet:** A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security.
- **Proprietary Information:** Proprietary information, also known as a trade secret, is information a company wishes to keep confidential. Proprietary information can include secret formulas, processes, and methods used in production.
- **Spam:** Irrelevant or inappropriate messages sent on the Internet to a large number of recipients.

7. Board Members Policy

Technology Resources

For purposes of this policy, "technology resources" means electronic communication systems and electronic equipment.

Availability of Access

Access to the District's technology resources, including the Internet, shall be made available to Board members primarily for official duties and in accordance with administrative regulations.

Limited Personal Use

Limited personal use of the District's technology resources shall be permitted if the use:

1. Imposes no tangible cost on the District; and
2. Does not unduly burden the District's technology resources.

Acceptable Use

A Board member shall be required to acknowledge receipt and understanding of the user agreement governing use of the District's technology resources and shall agree in writing to allow monitoring of their use. Noncompliance may result in suspension of access or termination of privileges. Violations of law may result in criminal prosecution.

Monitored Use

Electronic mail transmissions and other use of the District's technology resources by a Board member shall not be considered private. The Superintendent or designee shall be authorized to monitor the District's technology resources at any time to ensure appropriate use.

Disclaimer of Liability

The District shall not be liable for a Board member's inappropriate use of technology resources, violations of copyright restrictions or other laws, mistakes or negligence, and costs incurred. The District shall not be responsible for ensuring the availability of the District's technology resources or the accuracy, appropriateness, or usability of any information found on the Internet.

District Signature_____ Date_____

Signature Student/Employee_____ Date_____