Hughes Springs Independent School District

Acceptable Use Policy

The term "user" and "users" in this document refers to any persons using Hughes Springs Independent School District (HSISD) technology resources, whether they are a staff member, student, or any other affiliate of HSISD.

Introduction

Hughes Springs ISD recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop modern technology and communication skills.

Within our commitment to these skills, HSISD may provide Internet access, desktop computers, mobile computing devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more to users. The policies outlined in this document are intended to cover *all* available technologies, not just those specifically listed.

This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or personally-owned devices on campus or for any other school function.

All users are expected to use good judgment and to follow the specifics of this document as well as the intent in which it is written: be safe, appropriate, careful and kind; do not try to get around technological protection measures; use good common sense; ask if you're unsure.

General Usage

- All resources provided by HSISD are intended for educational purposes. Any use of resources not in support of HSISD's educational goals is prohibited.
- All activity on the HSISD network, District devices, or other technology services, including cloud services, may be monitored and retained for security, discipline, record keeping, and analytical reasons.
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- Hughes Springs ISD makes a reasonable effort to ensure students' safety and security online but will not be held accountable for any harm or damages that result from use of school technologies.
- Any modifications, unauthorized by the Technology Department, that harm the integrity of HSISD systems can result in disciplinary action for the user and potential financial responsibility.
- Users of any District resources or personal devices while within the District are expected to alert the campus office and/or the I.T. staff immediately of any concerns for safety or security.

Computing Devices

Hughes Springs ISD may provide users with computing devices to promote learning/productivity inside and outside the classroom setting. These devices should be brought to school with the student or staff member every day they report to school. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network. School-issued devices may be monitored outside of the school network. Any violation of school policy or misuse of school resources regardless of physical location may result in disciplinary action.

Users are expected to treat these devices with extreme care and caution; these are expensive resources that the school is entrusting to the user's care. It is the responsibility of the user to bring the device to school charged; the school is not responsible for or expected to provide charging options for devices. Users should report any loss, damage, or malfunction to teacher, campus office, or I.T. staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse as determined by the Technology Department.

Personally-Owned Devices / Bring Your Own Device

Students with personally-owned devices (including, but not limited to, laptops, tablets, smart phones, and cell phones) are encouraged to use their devices in support of their learning if their teacher grants them permission to do so or other campus rules allow such use. Otherwise, the devices should be turned off and put away during school hours unless in the event of an emergency.

During the school day, no device may be used to record, store, or transmit any type of image, sound, or video, except for approved projects with the express permission of the teacher of the class the student is attending at the time of the recording.

It is the responsibility of the user to bring the device to the school charged; the school is not responsible for or expected to provide charging options for devices.

Campus personnel or the Technology Department may deny usage of personal devices to any user due to misconduct or if the device is deemed a security threat to the District or other users. Devices may be confiscated if in violation of HSISD policies, including this. Return of the device is contingent on offense and/or handbook guidelines.

Because of security and content concerns, students are not allowed to use their own cellular or any other connection to access the internet or other data sources. Student-owned devices must be connected to the HSISD wireless network designated for them. Staff-owned devices should be connected to the HSISD wireless network designated for them especially when using the device for instructional purposes. For information regarding which network(s) are appropriate to connect to, contact your campus office or the Technology Department.

HSISD is not liable, financially or otherwise, for damages or repairs resulting from personal device usage.

Internet Access

Hughes Springs ISD provides its users with access to the Internet, including web sites, resources, content, and online tools. Access to online content may be restricted and/or censored in accordance with HSISD policies and federal regulations, such as the Children's Internet Protection Act (CIPA). Web browsing may be monitored and web activity records may be retained indefinitely.

Users should respect that the web filter is a safety precaution and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow District protocol to submit the site for review.

Email

Hughes Springs ISD may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

If users are provided with email accounts, they should be used with care. Hughes Springs ISD has chosen not to limit students' capabilities to communicate with organizations across the country including colleges, testing institutions, scholarship opportunities, etc. With this capability there is a need to emphasize that **email capabilities provided by HSISD are for school use only.** Any non-educational communication could be removed without warning and could result in disciplinary action. Users should not send personal information; should not use their school email account to conduct or promote commerce; should not use their school email address in association with third party services for personal use like Amazon, Facebook, iTunes, etc.; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the District policy or the teacher. If you are not completely sure an email or attachment is safe to open, consult the Technology Department for assistance.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage will be monitored and archived for a minimum of 10 years in accordance with state and federal law.

Online Storage

Staff members and some students will have access to online storage allowing them to access their files and shared files on any device anywhere. This brings unique opportunities to teaching staff and students to continue the learning process outside the classroom. As with email, users should only use this resource for school purposes. Any content found to be without educational value or of malicious intent will be removed without the user's consent. Users found to be storing such content could be subject to disciplinary action.

HSISD does not directly backup or archive data hosted in the online platform. Instead, HSISD utilizes fault tolerances built into the platform. Upon leaving HSISD, it is the user's responsibility to secure copies of their personal data outside of the cloud platform before their last date of attendance at HSISD.

Users may not use any online storage platform other than that which is provided by the district to store files and data containing information concerning students or staff members. Doing so may be in violation

of State and Federal law and could result in discipline, termination, and/or criminal charges.

Web Based Collaborative Content

Recognizing the benefits collaboration brings to education, Hughes Springs ISD may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Due to information security concerns, staff members shall not use any online resources or software which require user registration or gather any type of user-specific usage data without the written consent of the Director of Technology. The Director of Technology will evaluate the information security practices as well as the information used and stored by the third party and allow or deny usage based on these findings.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, and messaging may be monitored and archived. Users should be careful not to share personally-identifying information online.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should also recognize that among the valuable content online there is also unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn't want parents, teachers, future colleges, or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways never intended.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Do not be mean. Do not send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that online activities are monitored and retained.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author. Contact instructional staff for more information on properly citing research.

Network Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs, and not opening files or programs of unknown or untrusted origin.

If a user believes a computing device might be infected with a virus, malware, or other types of malicious software, the user should turn off the device and alert the Technology Department immediately. Users should not attempt to remove the virus or download any program to remove the malicious content.

Software Downloads and Installation

Users should not download, install, or execute any program over the school network or onto school resources without express permission from the Technology Department.

Users may download other file types, such as images or videos. For the security of the HSISD network, download such files only from reputable sites, and only for education purposes.

Personal & Information Security

Users should never share personal information including user accounts, passwords, phone numbers, addresses, social security numbers, birthdays, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission.

HSISD I.T. personnel may ask for username and password information while assisting with problems and should only do so in person or over the HSISD phone system. Do not share this information with anyone other than members of HSISD I.T. staff. Requests for login information by any person other than HSISD Technology Department personnel should be handled as an attempted system breach and reported to the Technology Department immediately.

If a user ever encounters a message, comment, image, or anything else online that causes concern for their own or another users personal safety, bring it to the attention of an adult (teacher or staff if at school; parent if using the device off-campus) immediately. HSISD staff should bring any such concerns to I.T. staff immediately.

Data Classification and Handling

Data classification and handling provides a framework for classifying and securing data based on the associated risks, as well as for applying the appropriate levels of protection as required by State and/or Federal law taking into consideration proprietary, ethical, operational, and privacy concerns. All HSISD data, whether electronic or printed, should be categorized within these criteria. It is the responsibility of all HSISD users to protect their own information as well as any other data they may access as part of their duties or accessed inadvertently. These classification and handling procedures apply to all data owned and managed by HSISD.

Definitions:

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, cellular devices, notebook computers, tablet computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers, and service bureaus and the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information on those resources.

Data Owner: Persons assigned the responsibility of approving user accounts and granting access rights to a specific data set within an Information Resource by its System Owner. There may be multiple Data Owners within an Information Resource, but there will be only one Data Owner for a defined data set. The System Owner will be responsible for managing the use of Data Owners, applicable forms and rules to be followed.

Sensitive Personal Information (SPI): An individual's first name or first initial and last name in combination of any one or more of the following items, if the name and the items are not encrypted.

- Social security number;
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Information that identifies an individual and relates to:
    - The physical or mental health or condition of the individual;
    - The provision of health care to the individual;
    - Payment for the provision of health care to the individual.

Personally Identifiable Information (PII): Information that alone or in conjunction with other information identifies an individual, including an individual's:

- Name, date of birth, or government-issued identification number;
- Mother's maiden name;
- Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
- Unique electronic identification number, address, or routing code; and
- Certain telecommunication access device as defined by regulation

Family Educational Rights and Privacy Act (FERPA) Protected Information: Any information not determined to be directory information by HSISD must be consented to by the student's guardian or student of legal age prior to release. Examples include:

- Any SPI or PII data elements
- Grade Point Average/Letter Grades
- Academic Standing
- Indication of Financial Aid Status
- Counseling records
- Academic Comments

General Information: Any information that is not related to SPI, PII, and/or FERPA or not otherwise protected by regulation(s) and/or publicly available. This information will include most directory information. Examples include a person's:

- Name along with residential address and/or telephone numbers.

- Email address
- Age and Sex
- Title or Position

SPI DATA HANDLING POLICY:

- All SPI data elements must be encrypted upon removal from source repository.
- All SPI data should be stored in locations only accessible by the user or other users who are permitted to view SPI data.
- All SPI must be purged as soon as reasonably possible if residing outside source repository.
- SPI information is only allowed to be transferred from the source repository to an HSISD managed device or an approved third party.
- Only individuals authorized by the Superintendent or Technology Director may have access to SPI.
- Process in place to audit information resources that contain SPI data must be followed.
- Access to SPI data will only be granted by the data owner or designee.
- SPI data transmitted over public networks must be encrypted.
- If any SPI data is processed and/or stored by a third-party, the third-party must be evaluated by the Technology Director.
- Any agreements with third parties that involve SPI data must be assessed by the Technology Director.
- Any employee that suspects SPI data has been compromised, lost, or otherwise disclosed without authorization must disclose the incident immediately to their supervisor, Technology Director, and Superintendent.

PII DATA HANDLING POLICY:

- Any PII data element alone or in combination must have the approval of the data owner, application manager, or Technology Director prior to being accessed from the source repository.
- All PII data should be stored in locations only accessible by the user or other users who are permitted to view PII data.
- Any record and/or document with more than 3 PII data elements must be encrypted prior to being transmitted and/or stored on public networks.
- PII data stored outside the source repository must be purged as soon as reasonably possible.
- PII information is only allowed to be transferred from the source repository to an HSISD managed device or an approved third party.
- If any PII data is processed and/or stored by a third-party, the third-party must be evaluated by the Technology Director.
- Any agreements with third parties that involve PII data must be assessed by the Technology Director.
- Any employee that suspects PII data has been compromised, lost, or otherwise disclosed without authorization must disclose the incident immediately to their supervisor, Technology Director, and Superintendent.

FERPA PROTECTED DATA HANDLING POLICY:

- All FERPA protected data elements, alone or in combination, must have the approval of the data owner, application manager, or Technology Director prior to being accessed from the source repository.
- All FERPA data should be stored in locations only accessible by the user or other users who are permitted to view FERPA data.
- Any FERPA protected data element that can be easily associated with the individual student must be encrypted prior to being transmitted and/or stored on public networks.
- FERPA protected data stored outside the source repository must be purged as soon as reasonably possible.

- FERPA information is only allowed to be transferred from the source repository to an HSISD managed device or an approved third party.
- If any FERPA data is processed and/or stored by a third-party, the third-party must be evaluated by the Technology Director.
- Any agreements with third parties that involve FERPA data must be assessed by the Technology Director.
- Any employee that suspects FERPA data has been compromised, lost, or otherwise disclosed without authorization must disclose the incident immediately to their supervisor, Technology Director, and Superintendent.

Failure to comply with these data handling guidelines may be in violation of State and Federal law and could result in discipline, termination, and/or criminal charges.

Limitation of Liability

Hughes Springs ISD will not be responsible for damage or harm to persons, data, or hardware while using technology resources.

While Hughes Springs ISD employs content filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Hughes Springs ISD will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Examples of Acceptable Use

I will:

- ✓ Use technologies at school for school-related purposes and activities.
- ✓ Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- ✓ Treat school resources carefully, and alert staff if there is any problem with their operation.
- ✓ Encourage positive, constructive discussion when allowed to use communicative or collaborative technologies.
- ✓ Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- ✓ Cite sources when using online sites and resources for research.
- ✓ Recognize that use of school technologies is a privilege and treat it as such.
- ✓ Be cautious to protect the safety of myself and others.
- ✓ Help to protect the security of school resources.

This is not intended to be an exhaustive list. Users should use good judgment when using technologies at school.

Examples of Unacceptable Use

I will **not**:

- ✓ Use technologies at school in a way that could be personally or physically harmful.
- ✓ Attempt to find inappropriate images or content. This includes: viewing, posting, or distribution of messages that are obscene, vulgar, profane, harassing, sexually oriented, sexually explicit, pornographic, offensive to others, or threatening to others.
- ✓ View or participate in social network sites or chat rooms other than those sponsored and overseen by the District.
- ✓ Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- ✓ Try to find ways to circumvent the school's safety measures and filtering tools or tamper with anyone else's computer, files, or email.
- ✓ Use technologies at school to send spam or chain mail. This includes: forgery of electronic mail messages or transmission of unsolicited junk email chain messages.
- ✓ Plagiarize content I find online or engage in unauthorized use of copyrighted material, including violating District software licensing agreement(s)
- ✓ Install any personal software on District equipment without approval of the Technology Department.
- ✓ Engage in unauthorized disclosure, use, or distribution of personal identification information regarding students or employees.
- ✓ Engage in personal political use to advocate for or against a candidate, office-holder, political party, or political position, measure, or proposition. (Such activity is not a violation when fulfilling an assignment for course credit.)
- ✓ Agree to meet in real life someone I met online.
- ✓ Use language online that would be unacceptable in the classroom.
- ✓ Engage in use that violates the applicable code of conduct or handbook.
- ✓ Use technologies at school for illegal activities, pursue information on such activities, or engage in any use that would be unlawful under state or federal law.
- ✓ Attempt to hack or access sites, servers, or content within the District's network or outside it that is not intended for my use.
- ✓ Engage in use related to commercial activities or for commercial gain.
- ✓ Advertise for purchase or sale of a product.

This is not intended to be an exhaustive list. Users should use good judgment when using technologies at school.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Notification to parents
- Detention or suspension from school and school-related activities
- Incur consequences under the school's Student Code of Conduct or handbook
- Incur consequences under the Employee Handbook
- Legal action and/or prosecution

Page Intentionally Left Blank

I have read and understood this Acceptable Use Policy and agree to abide by it:

_____

User Printed Name

_____ _____

User Signature Date

IF FOR A STUDENT: I have read and discussed this Acceptable Use Policy with my student:

_____

Parent/Guardian Printed Name

_____ _____

Parent/Guardian Signature Date