Hughes Springs Independent School District
Acceptable Use Policy for Students

The term "user" and "users" in this document refers to any student using Hughes Springs Independent School District (HSISD) technology resources.

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 are 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.
- Users 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 usage, unauthorized by the Technology Department, that harms the integrity of HSISD systems can result in disciplinary or legal 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 provides computing devices to promote learning and productivity inside and outside the classroom setting. 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. Users should report any loss, damage, or malfunction to a teacher, campus office, or I.T. staff immediately. Users may be financially accountable for any damage resulting from abuse or negligence.

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. Any violation of school policy or misuse of school resources regardless of physical location may result in disciplinary action.

Additional policies pertaining to devices issued to students through 1:1 programs are found in the HSISD 1:1 Student Device Handbook available on the school's website.

Personal Devices / Bring Your Own Device

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

Due to security and content concerns, students are not permitted 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. For information regarding which network(s) are appropriate to connect to, contact your campus office or the Technology Department.

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. Return of the device is contingent on offense and/or handbook guidelines.

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

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.

Electronic Communication

Hughes Springs ISD provides some students with email accounts and other communication platforms for the purpose of school-related communication. Availability and use may be restricted based on school policies.

If students 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, use their school email account to conduct or promote commerce, or use their school email address in association with third party services for personal use like Amazon, Facebook, iTunes, etc., or attempt to open files or follow links from unknown or untrusted origin. 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. Electronic communications will be monitored, and email archived for a minimum of 10 years in accordance with state and federal law.

Online Storage

Some users will have access to online storage allowing them to access their files and shared files on any device anywhere. This brings unique opportunities 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 back up 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.

Internet Etiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner. Users are expected to communicate in any online platforms 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.

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 would not want parents, teachers, future colleges, or employers to see. Once something is online, it can be shared and spread in unintended ways.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. 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 content (or use as their own, without citing the original creator) including words or images from the Internet. Users should not take credit for things they did not 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 users engage in practices that could potentially harm the HSISD network and associated services, whether intentional or accidental, users may be subject to mandatory training and/or account suspension. In the event of account suspension, the user is still responsible for completing all required assignments. Revocation of computer privileges will not be an acceptable excuse for late work.

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 met online in real life without parental permission.

HSISD Technology 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 Technology 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 encounters a message, comment, image, or anything else online that causes concern for their own or another user's personal safety, bring it to the attention of an adult immediately.

Application account management for students under 13

The Children's Online Privacy Protection Act (COPPA) is a federal law that regulates the online collection of personal information from children under the age of 13. The law generally requires website operators to provide parental notification and obtain parental consent before collecting personal information from these students. However, COPPA also authorizes school districts to provide this consent when the collection of information is for the use and benefit of the school and for no other commercial purpose. Parents can obtain more information regarding COPPA via the Federal Trade Commission website at www.ftc.gov. HSISD recommends and/or manages certain web-based applications that have been vetted for appropriateness, compliance with federal privacy laws (FERPA), and educational value to enhance the learning experience of students. In compliance with COPPA, HSISD manages student accounts and logons for these resources. Managing these accounts may require the disclosure of certain basic information about students such as name and school name.

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.

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
- Consequences under the school's Student Code of Conduct or handbook
- Legal action and/or prosecution

Acceptable Use Policy Agreement

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.
- ✓ Engage in 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.

I will **not**:

- ✓ Use technologies at school in a way that could be personally or physically harmful.
- ✓ Agree to meet in real life someone I met online.
- ✓ Use language online that would be unacceptable in the classroom.
- ✓ Attempt to find inappropriate images or content online.
- ✓ View or participate in social network sites or chat rooms other than those approved by the District.
- ✓ Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- ✓ Attempt to circumvent the school's safety measures and filtering tools or tamper with anyone's computer, files, or email.
- ✓ Attempt to hack or access private or confidential sites, servers, or content inside or outside the District.
- ✓ Plagiarize content I find online or engage in unauthorized use of copyrighted material.
- ✓ Install personal software on District equipment without approval of the Technology Dept.
- ✓ 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.
- ✓ Use school technology to advocate for or against a candidate, officeholder, political party, or political position, measure, or proposition, unless fulfilling an assignment for course credit.
- ✓ Use technologies at school to send spam or chain mail.
- ✓ Engage in use related to commercial activities or for commercial gain.
- ✓ Engage in use that violates the Student Code of Conduct or Student Handbook.

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

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

User Printed Name

User Signature Date

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

Parent/Guardian Printed Name

Parent/Guardian Signature Date