-Staff-
Acceptable Use Policy
for District Technology Resources

The district has certain measures in place to keep students and staff safe, legal, and responsible. The policies outlined here apply to all SSISD computer networks (including the devices made available to them), and all devices connected to those networks (whether on district grounds, or off). SSISD will provide access to help staff connect on a global scale, but this brings great responsibility. It is your responsibility to follow all rules for appropriate use. Board Policy CQ (Local), the Sulphur Springs ISD Employee Handbook, Student Code of Conduct, and the Student Handbooks require or reference acceptable use policies and agreements for all users.

Please note that the Internet is a network of many types of communications and information networks. It is possible that you may run across some material you might find objectionable. While SSISD uses filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use and any efforts to circumvent the safeguards in place are prohibited. As a staff member, you have more access than a student. Use it carefully, thoughtfully, and review each source of content before displaying content to students. Use of, or support of student use of, tools like Mobile Air Cards or Mobile Hot Spots are strictly forbidden within district facilities and may result in disciplinary action when discovered.

Please contact the Technology Department if you have questions or need help understanding this material.

Inappropriate use of the district's technology resources may result in suspension or revocation of the privilege of using these resources, as well as other disciplinary or legal action, in accordance with applicable district policies, administrative regulations, and laws.

Responsible Use

Any use described below is deemed **"responsible**." The final decision regarding whether any given use of the network or internet is acceptable lies with the Superintendent or designee.

- Use is for educational reasons, but some limited personal use is permitted by policy
- Messages sent with the accounts provided infer that your messages represent the district's point of view
- Use supports the educational and administrative purposes, goals, and objectives of SSISD
- Use is limited to your individual account and your assigned devices – you and only you should use your assigned account, **and you should never share your password with others, for any reason.**
- Use furthers research related to education and instruction
- Use does not violate any policies or handbooks
- Maintain the confidentiality of health or personal information concerning colleagues and students, unless disclosure serves lawful professional purposes or is required by law
- Before using a district device or for a district purpose, digital subscriptions, online learning resources, online applications, or any other program must be approved by the Curriculum and Technology Departments via the Curriculum & Technology Request Form
- Practice only sending information that can be viewed by anyone which lowers the risk of sending information that is sensitive or confidential, and could be requested through the Freedom of Information Act (FOIA)

Unacceptable and Irresponsible Use

Any of the following uses is deemed "**Unacceptable and Irresponsible**." This list **does not include all** possible violations. The final decision regarding whether any given use of the network or internet is acceptable lies with the Superintendent or designee.

Disciplinary action may be taken for unacceptable and irresponsible use of the network or Internet.

- Use of school technology resources to encourage illegal behavior or threaten school, staff, or student safety
- Sending or posting messages and/or content that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal
- Use of any means to disable or bypass the district's Internet filtering system or other security systems
- Attempting to or enabling others to destroy, disable, or gain access to district technology equipment, district data, the data of others, or other networks connected to the district's system, including uploading or creating computer viruses or reckless programs and scripts of any sort
- Encrypting communications or files to avoid security review
- Posting personal information about yourself or others (such as addresses and phone numbers) other than as needed to conduct school operations
- Using devices or accounts that are not assigned to you
- Unapproved use of social technology resources such as chat rooms, sites, and games
- Forgery of e-mail messages or transmission of unsolicited junk e-mail
- Unauthorized use of copyrighted material, including violating district software licensing agreements
- Use related to commercial activities or for personal commercial gain
- Use that violates the employee handbook, or is unlawful
- Accepting terms and conditions or signing user agreements on behalf of the district without preapproval
- Use of an AI or generative application that does not align with district policies or to perform any other activity that would also violate district policies
- Use of an AI or generative application, or any other applications use is prohibited when in violation of district policy, the employee handbook, and/or used in perpetuating bias or misinformation, or breaching student privacy
- Wasting school resources through the improper use of the computer system

Consequences for Inappropriate Use

One or more of the following consequences may be imposed:

- Suspension of access to the system
- Revocation of the network or online account(s)
- Removal of device access
- Other action, including disciplinary action, in accordance with board policy and/or the employee handbook as applicable

Internet Safety

Safe Online Communication – Online communication is important but not without some risk. While the

district will work to keep users out of risky situations, users must also do their part in avoiding risky online behavior. Staff should recognize and avoid inappropriate communications and report anything out of the ordinary to campus or district administration. Never share passwords, personal information, or inappropriate photos of yourself or others.

Internet Privacy – Be aware of online applications and websites as they may collect user information for various reasons which could put your information at risk. Take measures to omit or limit personal information and have a general understanding of how companies and websites collect information based on their privacy terms.

Research and Information Literacy

AI - Sulphur Springs ISD recognizes that artificial intelligence tools are increasingly accessible to both students and staff. Staff may use AI tools to support instructional and professional responsibilities; however, AI may not replace professional educator judgment, and all AI-assisted work requires meaningful human review prior to implementation or use with students. Staff must never enter personally identifiable student information into non-district-approved AI tools, as doing so may constitute a FERPA violation. All use of artificial intelligence on district devices, networks, or in connection with district work must align with applicable laws, district policies, and academic integrity standards.

Searching – Staff will determine validity of information and use materials correctly. Staff will use search engines, and other searching methods, to find information and content and utilize cybersecurity best practices while accessing resources.

Research and Evaluation - Staff will learn how to evaluate applications, websites, and digital resources for credible information. They'll use multiple sources to confirm information, and they will preview and confirm any resource that will be displayed to students prior to student access. Staff will also be able to identify online advertisements and spam and understand their purpose and methods of avoidance.

Technology use of district resources IS NOT PRIVATE and may be viewed by district officials. All district provided accounts are to be used for educational purposes and adhere to responsible use guidelines and acceptable use policies. SSISD will monitor activity involving district equipment and services.

Accounts

The district uses various technology tools throughout the school year that require accounts and student data to be collected. In such cases, campus or district staff will verify adherence to the Children's Online Privacy Protection Act (COPPA) and Family Educational Rights and Privacy Act (FERPA) before creating anything on behalf of the students. The district will keep a current list of approved and unapproved tools on the district technology website for staff, students, and parents to view. This list will be updated throughout the year as tools are reviewed and new tools are included. All tools will be reviewed using an established district process.

Devices

The district provides staff members in the district with digital devices. Staff are expected to keep their devices clean, in proper working order, and address any issues promptly with the technology support for their campus. Staff issued devices are SCHOOL PROPERTY and are required to be returned in working order.