Spring Hill Unified School District

Student Acceptable Use Policy

General Statement of Policy

Spring Hill Unified School District provides access to the district computer network and computing devices (district technology) for intranet resources, e-mail and the Internet. Access to the Internet enables students to have access to electronic information that enables them to explore thousands of libraries, databases, educational resources, participate in distance learning and communicate with experts and other Internet users around the world. Access to the Internet through the district network is provided for educational and professional use to enable students to achieve greater academic and future success.

Spring Hill Unified School District is committed to making advanced technology and increased access to learning opportunities available to students, faculty, and other district employees. The district's goal in providing this access is to promote educational excellence in schools by facilitating resource sharing, innovations, and communications. To be in compliance with the Children's Online Privacy Protection Act (COPPA) and the Kansas Children's Internet Protection Act (KS-CIPA) as mandated by Congress and KS State Statute 75-2589, Spring Hill Unified School District has implemented the following guidelines and procedures for using the Internet.

This Acceptable Use Policy and Media Consent form is a legally binding document.

CIPA mandates school districts to certify that they have an Internet Safety Policy in place. These mandates and assurances must be in place so the district can receive E-rate funds or funds under Title III of Elementary and Secondary Education Act of 1965.

Spring Hill Unified School District incorporates Internet filtering technology, remote monitoring technology, network transaction auditing and staff supervision to prohibit obscenity, child pornography and material harmful to minors in compliance with CIPA.

COPPA applies to the online collection of personal information from children under 13. School districts must be COPPA compliant to receive E-rate funds. Spring Hill Unified School District does not disclose personal information about students on district websites or through any unsecured Internet communication and staff members are instructed not to allow students to enter personal information on any external website or through any other Internet communication to comply with COPPA. A consent form must be signed prior to any personal student information or work being placed on any district provided website.

Limited Educational Purpose

With access to computers and people all over the world comes the potential for access to material that is illegal, defamatory, inaccurate or offensive to some people. The school district system has a limited educational purpose, which includes use of the system for classroom activities, professional or career development, and limited high-quality self-discovery activities. Users of the system are expected to use the Internet to further educational and personal goals consistent with the mission of the school district and school policies. Uses that might be acceptable on a user's private personal account on another system may not be acceptable on this limited purpose network.

Spring Hill Unified School District has taken steps to restrict access to inappropriate resources and information on the network and to monitor student use of the network. However, on a global network it is impossible to effectively control student access to all inappropriate material. The primary responsibility for access will rest with the student. We believe that the benefits to students through access to the Internet exceed the potential disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying standards that children should follow when using media and information sources. To that end, Spring Hill Unified School District supports and respects each family's right to decide whether or not to apply for district network access. Alternate resources will be provided for children who do not have permission to access the Internet.

Use of District-owned Technology is a Privilege

The use of school district technology is a privilege, not a right. All users are responsible for good behavior on school computer networks and computing devices just as they would be if in a classroom. General school rules for behavior and communication apply. Authorized district personnel may review student/user files and communication to prevent misuse and to ensure students are using district technology responsibly and in compliance with applicable laws and district policies. There is no expectation of privacy when using technology resources owned and/or provided to users through Spring Hill Unified School District. Depending on the nature and degree of the violation and number of violations of the district policy, unauthorized or improper use of the school district technology or the Internet may result in one or more of the following consequences: suspension or cancellation of use of access privileges; payments for damages or repairs; discipline under other appropriate school district policies, including suspension and/or expulsion; and/or civil or criminal liability under applicable laws. In order to provide guidance, the following pages contain a non-comprehensive list of unacceptable uses and student rights. Please read these carefully. The district retains broad discretionary authority to maintain safety, order and discipline regarding unauthorized and improper use of these resources.

The following guidelines govern the use of the district network and computers:

District Technology

- Student shall not use district-owned technology for illegal nor inappropriate uses at any time. The district network refers to the network provided on school grounds for educational use. The guidelines for district-owned computers cover use both at school and away from school.
- Student is responsible for the proper use and care of district technology in their use or possession. This includes all classroom technology, computer lab technology, and district-owned personal computing devices loaned to the student.
- Student who has been loaned a district computing device shall abide by the requirements of the Loan Agreement and the Damage/Loss Program.

Student Internet Access

- All students may have access to the school district network and the Internet's information resources and are responsible for the ethical and responsible use of these resources. Although monitored by school officials, ultimately, parents and guardians of minors are responsible for setting and communicating the standards that their children should follow when using media and information sources.
- Students may have e-mail access through a district e-mail account. This resource is for academic uses only and may be monitored to ensure responsible use. Personal e-mail accounts should not be accessed while using the district network. Appropriate use of personal e-mail is required on all district computing devices.
- Students may utilize the following educational websites for academic uses: Adobe (https://adobe.com), Amplify (https://amplify.com), AP Classroom (https://myap.collegeboard.org/), Apple Classroom (https://www.apple.com/), Autodesk Fusion 360 (https://www.autodesk.com/products/fusion-360/), Cengage (https://www.cengage.com/mindtap), CK-12 (https://www.ck12.org), Clever (https://clever.com), Code (https://code.org), ConnectEd (https://connected.mcgraw-hill.com), Delta Math (https://www.deltamath.com), Desmos (https://www.desmos.com), E-hallpass (http://eduspiresolutions.org/), EdPuzzle (https://edpuzzle.com), EverFi (https://everfi.com), Fastbridge (https://www.illuminateed.com/), FlipGrid (https://info.flip.com), Foundations U (https://www.foundationsu.com/high-school), Geogebra (https://www.geogebra.org), Gizmos (https://www.explorelearning.com), Go Formative (https://goformative.com), Google for Education (https://edu.google.com), HMHCO (https://www.hmhco.com), iCivics (https://iCivics.org), Kahoot (https://kahoot.it), Khan Academy (https://www.khanacademy.org), Microsoft Office 365 (www.office.com), Mystery Science (https://mysteryscience.com), Nearpod (https://nearpod.com), Newsela (https://newsela.com), Nitro Type (https://nitro type.com), Pearson Savvas Realize (https://www.savvas.com), PebbleGo (https://pebblego.com), Quizlet (https://quizlet.com), Quizziz (https://quizizz.com), Read Live (https://readlive.readnaturally.com), Rosetta (https://www.rosettastone.com), Seesaw (https://web.seesaw.me), Sora ebooks (https://www.overdrive.com/), STEMscopes (https://acceleratelearning.com/), Sutori

(https://www.sutori.com), TinkerCAD (https://www.tinkercad.com), Typing Club (https://www.typingclub.com), Xello (https://xello.world/en/)

- Student use of district network to access social networking sites, such as, but not limited to, Twitter, Instagram, Facebook and/or Snapchat, is prohibited, except for academic and extra-curricular school activities. Student/teacher interaction on Facebook and other social networking sites should not contain personal communication and are for dissemination of school information only. Student/teacher interaction on personal social networking accounts must be appropriate and public.

Personal Safety

- Student shall not post personal contact information about himself/herself or other people online. Personal contact information includes your address, telephone number, school address, work address, etc.
- Student shall not agree to meet someone he/she met online without parent's approval and participation. Parent should accompany student to the meeting.
- Student shall promptly report to a teacher or other appropriate school employee any message received that is inappropriate or makes him/her uncomfortable.
- Students shall immediately report to a staff member any obscene, pornographic or offensive material found.
- Instructional staff will educate students about appropriate online behavior, including interactions with other individuals on social networking sites/chat rooms, and cyber bullying awareness and response.

Illicit Activities

- Student will not attempt to gain access to the district network or to any other computer system that is not authorized. This includes attempting to log on though another person's account or access another person's files. These actions are illegal, even if only for the purpose of "browsing."
- Student shall not make deliberate attempts to disrupt the computer network or destroy data by spreading computer viruses, loading illegal files, or by any other means. These actions are illegal.
- Student shall not post, publish, or display harmful material that is threatening, obscene, disruptive, bullying, sexually explicit, or that harasses others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Student shall not use district technology to engage in illegal commercial or for-profit activities.
- Student shall not use district resources to solicit, create, forward, or reply to any email that could be classified as a chain letter or SPAM.

System Security

- Student is responsible for his/her network account and should take all reasonable precautions to prevent others from being able to use the account. Except when working directly with USD 230 staff you should not provide your password to another person.
- Student shall immediately notify a teacher, school administrator, librarian or district technology department if he/she has identified a possible security problem. Do not go looking for security problems; this may be construed as an illegal attempt to gain access.
- Student shall not download software or install programs unless it is authorized by the district.
- Student shall do nothing to disrupt the use of the system for others, including changing programs or files, modifying settings, changing passwords, or reconfiguring the system.
- Student shall not physically modify, harm, or destroy any computer or network hardware in any manner.
- Any student identified as a security risk may be denied access.

Inappropriate Language

- Restrictions against inappropriate language apply to public messages, private messages, and material posted on web pages.
- Student shall not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- Student shall not post information that could pose a threat of danger or disruption.

- Student shall not engage in personal attacks, including prejudicial or discriminatory attacks, cyber-bullying, intimidation, hazing or other conduct that causes or threatens to cause bodily harm or emotional suffering.
- Student shall not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If you are told by the person to stop sending messages, you must stop.
- Student shall not knowingly or recklessly post false or defamatory information about a person or organization.

Respect for Privacy

- Student shall not re-post or forward a message that was sent to you privately without the permission of the person who sent you the message.
- Student shall not post private information about another person.
- Student shall not access another individual's materials, information or files without permission.
- Student shall not use someone else's password, user account, or logon information.
- Student shall not gain unauthorized access to resources.

Respecting Resource Limits

- Student shall use the system only for educational and career development activities.
- Student shall not download and/or listen to radio streaming, video streaming, use any online telephone resource, or music and/or video sharing application except for educational purposes.
- Student shall not download or install any improper or unauthorized software. All software on district computers must be licensed and approved. Pirated software will not be tolerated.
- Student shall not intentionally waste district resources.

Plagiarism and Copyright Infringement

- Student shall not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
- Student shall respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by copyright. Reproduction of a work includes using the work in another written form or posting the work or portion of the work on the Internet. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should requests permission from the copyright owner. Copyright law can be confusing; if you have questions, you should ask your teacher.

Artificial Intelligence

- AI technology can be an excellent resource for enhancing learning and teaching experiences, but it must be used responsibly and ethically. Student shall ensure that any AI systems they use are age-appropriate and that they do not violate the privacy of other individuals. The use of AI for academic purposes should align with the district's curriculum and instruction goals. Additionally, student must use AI tools responsibly, avoiding any form of plagiarism or cheating.

Inappropriate Access to Material

- Student shall not use the district technology to access harmful matter or material that is profane or obscene (pornography), that advocates illegal acts, or advocates violence or discrimination towards other people (hate literature). This may include certain song lyrics and related materials.
- If student mistakenly accesses inappropriate information, he/she should immediately tell the teacher or school administrator in charge. This will protect against any claim that the student intentionally violated this policy.
- Parent/guardian should instruct student regarding additional material that they think would be inappropriate to access. The district fully expects that students will follow parents' instructions in this matter.

Privacy Rights

- You should be aware that computer files and communications on the district's network, computers and the Internet are not private or secure.
- Use of mobile wireless Internet devices including but not limited to Hotspots and MiFi's at school is prohibited. Appropriate use of cellular phones is acceptable.
- Student will limit the use of the network and computer resources to classroom activities, teacher-directed activities, library-related research, or career development. Use of the system for any other purpose, personal or otherwise, is prohibited unless authorized by the district.
- The district may monitor student's use of the Internet and the district's computer resources. Monitoring of the system may lead to discovery of violations of the Student Acceptable Use Policy, the district's disciplinary codes or the law. The district reserves the right to suspend the use of personal electronic devices.
- Parents/guardians have the right to request to see the contents of their student's files.

Violations

- Violating this policy may result in one or all of the following: restricting technology access; loss of technology access; disciplinary or legal action including, but not limited to, suspension and/or expulsion; criminal prosecution under appropriate local, state and federal laws; and/or assessment of the cost of damages to hardware/software.
- The district will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the school district network.
- In the event there is a claim that a student has violated this policy in his/her use of the school district computing device or network, student will be notified of the suspected violation and have an opportunity to be heard in the manner set forth in the district's conduct policy.
- Major violations of the district's Student Acceptable Use Policy may result in the loss of use of all computing equipment and Internet access. The student may be able to regain computing privileges as appropriate. If this occurs, the student will be given the opportunity to remove his/her school-related files.
- If the violation also involves a violation of the district's disciplinary code, it will be handled in a manner described in the district's disciplinary code. Additional restrictions may be placed on the student's use of their network account.
- The district has broad discretionary authority to maintain safety, order and discipline and to ensure a positive learning environment for students and staff.

Limitation of Liability

The district makes no warranties of any kind, either express or implied, that the functions or services provided through the school district network or computing devices will be error-free or without defect. The district will not be responsible for any claims, damages, or injury of any nature whatsoever, which users may suffer as a result, whether directly or indirectly, of any use of the school district network or computers, including, but not limited to, personal injury, emotional distress or suffering, or loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising from the unauthorized use of the school district resources, including, but not limited to, the purchase of products or services.

Student Internet Access Permission Form and
Student Acceptable Use Policy Agreement
(Required for all users)

I have read, understand, and have discussed the Spring Hill School District Student Acceptable Use Policy with my child regarding appropriate use of technology and the Internet. I agree to support and uphold the guidelines, and I understand that should my child commit any violation, disciplinary action may be taken. If the violation constitutes a criminal offense, appropriate legal action may be taken. I do understand that there is objectionable material available on the Internet and that by following the Acceptable Use Policy guidelines, my child should not be exposed to this material. I further understand that precautions to restrict improper access to offensive language, images, text or other media have been taken by Spring Hill School District but due to the global and fluid nature of the Internet, Spring Hill School District cannot assure me that my child will be denied access to all undesirable materials.

Student Name _____Grade_____

Parent Name_____

Signature of Parent/Guardian_____

Date _____

{Rev. 6/2023}