Stone County School District

INTERNET/TECHNOLOGY ACCEPTABLE USE POLICY
(AUP)

INTERNET ACCESS

Stone County School District (SCSD) provides the privilege of Internet access to district faculty, staff, students, and occasional guests. Each user, as well as a minor's parent or guardian, voluntarily agrees to release, hold harmless, defend, and indemnify, the Stone County School District, its officers, board members, employees, and agents, for and against all claims, actions, charges, losses or damages which arise out of the user's use of the SCSD network, but not limited to negligence, personal injury, wrongful death, property loss or damage, delays, non-deliveries, mis-deliveries of data, or service interruptions. SCSD will fully cooperate with local, state, or federal officials in any investigation related to illegal activities conducted through the user's Internet account.

Access will be restricted as required to comply with the Children's Internet Protection Act (CIPA). Web browsing may be monitored, and records retained to ensure compliance.

Users are expected to respect the web filter and shall not attempt to circumvent the filter when browsing the Internet. The determination of whether material is appropriate or inappropriate is based solely on the content of the material and the intended use of the material, not on whether a website has been blocked or not. If a user believes a site is unnecessarily blocked, the user should submit a technology work order to review the site or a "Request for Access" notification directly from the blocked page itself.

Each user acknowledges that the information available from other websites may not be accurate. Use of any of the information obtained via the Internet is at the user's own risk. Stone County School District makes no warranty of any kind, whether expressed or implied, regarding the quality, accuracy, or validity of the data on the Internet.

SCSD NETWORK RULES

- The person to whom an SCSD network account is issued is responsible at all times for its proper use.
- Any inappropriate use may result in the cancellation of the privilege of use, and/or disciplinary action. Consequences for any user who fails to comply with SCSD, and school guidelines may include paying for damages, denial of access to technology, ISD, suspension, expulsion, or other remedies applicable under the school disciplinary policy, and state or federal law.
- Any district employee who uses the SCSD network or any district device attached to it inappropriately is subject to disciplinary action, including dismissal.
- Under no conditions should an SCSD network user give their password information to another user nor allow another user to utilize their account unless speaking directly to a technology department employee who is assisting them.

TECHNOLOGY ACCEPTABLE USE POLICY

- Schools may supplement any provisions of the district AUP (Acceptable Use Policy), and may require additional parent releases and approvals, but in no case will such documents replace the district AUP.
- Users will immediately report to school district authorities any attempt by other network users to engage in inappropriate conversations or personal contact. Any non-standard software that is needed to perform a specific job function will need to be brought to the attention of the Technology Department. Those applications shall be the sole responsibility of that office and if the application interferes with any required programs, applications, and utilities, it should not be used and if in use, it may be disabled.

ACCEPTABLE USES OF TECHNOLOGY (not all inclusive)

- Use school technologies only for school-related activities and assignments.
- Follow the same guidelines for respectful, responsible behavior online that they are expected to follow offline, on or off campus.
- Handle school resources carefully and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Immediately alert a teacher, administrator, or other staff member if they see threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use district technologies at appropriate times, in approved places, for educational pursuits.

This is not intended to be an exhaustive list. Users should use their own good judgment when using SCSD technology.

UNACCEPTABLE USES OF THE TECHNOLOGY (not all inclusive)

- Violating any state and/or federal law (i.e., copyright laws).
- Using profanity, obscenity, or other language that may be offensive to others.
- Conducting or orchestrating personal attacks on other people, organizations, religions, or ethnicities.
- Accessing, downloading, texting, emailing, storing, or printing files or messages that are sexually explicit, obscene, or that offend or tend to degrade others. The administration invokes its discretionary rights to determine such suitability.
- Not respecting the privacy of a person by posting personal or sensitive contact information, such as work/home address, telephone, e-mail, photographs, or names, without obtaining prior permission from the person affected.
- Student information shall be posted only with written parent/guardian permission.
- Forwarding personal information or communication(s) without the author's prior consent.
- Using district provided Internet, on or off campus, for commercial purposes, financial gain, personal business, producing advertisement, business service endorsement, or religious or political lobbying is prohibited.
- Destroying or altering school or district files or personal files of another user.
- Unauthorized viewing or taking the files of another user.

FILTERING

DISCLAIMER: SCSD disclaims all liability for the content or accuracy of materials to which a student or employee may access while using the district's Internet service and for any harm or damages suffered as a result of the student or employee's Internet use. While the SCSD takes steps to protect users from inappropriate material, to intercept malicious actions directed toward its users, no filtering system is perfect. Those risks must be recognized and accepted by all users who sign the district's Acceptable Use Policy.

An Internet filter is in service for Stone County School District. This filter is a critical component of the SCSD network and is Children's Internet Protection Act (CIPA) compliant since it allows valuable educational online Internet access while restricting access to specific unwanted material in the categories listed below. In order to maintain CIPA compliance the district employs web filtering on all devices whether they are being used on or off campus and the same policies for its use apply regardless of location. Inappropriate use will be dealt with in accordance with the policies set for by the SCSD whether an offense occurs on or off campus. This is not, by any means, an all-inclusive list and additional content may be at the discretion of the administration.

- Pornography
- Gambling
- Illegal Drugs
- Online Merchandising (unrelated to district activities)
- Hate Speech
- Extreme Violence
- Criminal Skills
- Alternative Journals
- Other Undesirable Material as determined by district administration.

The web filter is updated on a daily basis in order to restrict access to the above items. Filtering is **not** a 100% foolproof way of limiting access to appropriate sites. Inappropriate sites are added to the Internet daily. Students must be supervised at all times by a staff member while using the Internet. Inappropriate use is logged along with the date/time and the IP address of the workstation making the request on and off campus.
Attempts to bypass the district's Internet filters is in violation of this Acceptable Use Policy and will be subject to disciplinary action that may include denial of access to technology, ISD, suspension, expulsion, termination of employment or other actions as determined by the administration, school disciplinary policy and state or federal law.

WORKSTATION\MOBILE DEVICE MONITORING

Data transferred and/or transmitted over the SCSD network and Internet connection can be monitored and recorded at any time and originating users can be held liable if their use of these services violates any established policy, regulation, or law. Any data stored on district-owned equipment may be archived and preserved by the district for an indefinite period. Such data includes, but is not limited to E-mail, text documents, video files, digital photographs, music, and other digital or electronic files. If a particular workstation\mobile device continues to try to connect to an inappropriate site, that device will be remotely monitored and the individual using that device will be reported to the principal of the school and the individual's parent/guardian may be notified. Illegal use of a proxy and/or breach of security may result in disciplinary action(s).

TECHNOLOGIES COVERED

SCSD may provide the privilege of Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, email, and more.

The Acceptable Use Policy applies to both district-owned technology equipment utilizing the SCSD network, the SCSD Internet connection, and/or private networks/Internet connections accessed from district-owned devices at any time or location. The AUP also applies to privately-owned devices accessing the SCSD network, the SCSD Internet connection, and/or private networks/ Internet connections while on school property or participating in school functions or events off campus. SCSD policies outlined in this document cover all available technologies now and in the future. Not just those specifically listed or currently available.

EMAIL

Employee and student district email is the property of SCSD. SCSD archives employee and student email. All email accounts are deleted (and removed from the archive) when the user leaves the district unless a valid request for retention is received ahead of time. Email may also be retained as required by a legal hold request. It is the responsibility of the employee and student to maintain this email account appropriately.

SCSD provides faculty, staff, and students in grades K-12 with email accounts for the purpose of school-related communication. Grades K-7 are only allowed to communicate with others within the Stoneschools.org domain. Grades 8-12 have access to information outside the district for purposes of conducting/completing school related activities only.

No personal communications or non-school related communications are allowed. Availability and use may be restricted based on school policies.

Users with district email accounts should use these accounts with care. Users should not send personal information, attempt to open files, or follow links from unknown or untrusted origins. Student users should also use appropriate language and should only communicate with other people as allowed by district policy, their teacher or campus administrator.

USING EMAIL WHILE ACTING AS DISTRICT REPRESENTATIVE

(Students, Teachers, Administrators, Directors, Managers, etc.)

Student use of personal email accounts to conduct school related business is prohibited. It is highly recommended that staff not use personal email accounts while in the performance of work related duties. Personal email accounts are a conduit for malware, viruses, phishing, and ransomware attacks and are a significant danger to the safety and security of the district's sensitive resources.

Any OFFICIAL communication, e.g., Teacher to Parent, Teacher to Student, Staff to Staff, must be conducted via the district provided e-mail system. This includes, but is not limited to, staff who guide extracurricular activities such as Clubs, Choirs, Bands, Athletics, and the like. These, and all other work-related communications, are archived during the school year for your protection.

SECURITY

Users are expected to take reasonable safeguards against the transmission of security threats over the SCSD network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. Users should never share personal or sensitive information without proper authorization. If you are unsure about what this means ask your teacher (for students) or a supervisor (if you are a staff member) for clarification.

If users believe a desktop computer, laptop, or other device they are using might be infected with a virus, they should alert the technology department immediately. Users should not attempt to remove the virus themselves or download any programs to help remove the virus. Downloading and installation of free virus\malware removal programs can in many cases do more harm than the virus itself.

ONLINE ETIQUETTE

(Netiquette)

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

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

Users should not post anything online that they would not want students, parents, teachers, future colleges or employers to see. Once something is online, it can never be completely retracted and can sometimes be shared and spread in ways the user never intended.

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 did not create themselves or misrepresent themselves as an author or creator of something found online. Information obtained via the Internet should be properly cited, giving credit to the original author.

PERSONAL SAFETY

Students should never share personal information, including 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 or others. Users should never agree to meet in person someone they meet online without parental permission.

If users see a message, comment, image, or anything else online that makes them concerned for their personal safety or the safety of someone else, they should immediately bring it to the attention of an adult (teacher or administrator if at school, a parent if using the device at home).

CYBER BULLYING

Cyber bullying, including but not limited to, harassing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking will not be tolerated. Users should not send emails or post comments with the intent to harass, ridicule, humiliate, intimidate, or harm the targeted individual and create for the targeted individual a hostile school environment.

Engaging in these behaviors or in any online activities intended to harm (physically or emotionally) another person, will result in disciplinary action. In some cases, cyber bullying can be a crime. Users should remember that online activities might be monitored and recorded.

All students will be educated about appropriate online behavior, including interacting with other people on social networking websites and in chat rooms, and cyber bullying awareness and response.

SOCIAL MEDIA

The SCSD has a policy addressing social media and it applies to all employees and students. By signing the Staff/Student/Parent/Guardian Technology Agreement, users are acknowledging they have read and agree to abide by the Social Media guidelines outlined in the district's Social Media Policy (page 32 of the Technology Handbook). Violations of the Social Media Policy are also considered violations of the Acceptable Use Policy.

LIMITATION OF LIABILITY

SCSD will not be responsible for damage or harm to persons, files, data, or hardware. While SCSD employs web filtering and other safety and security mechanisms and attempts to ensure their proper function, it makes no guarantees as to their effectiveness and users should have no expectation of privacy while using district resources.

SCSD will not be responsible or liable for, financially or otherwise, unauthorized transactions conducted over the SCSD network or its Internet service. Violations of this policy may have disciplinary consequences, including:

- Suspension of network, technology, or computer privileges
- Notification of parents
- ISD or suspension from school and school-related activities
- For employees, disciplinary action up to and including termination of employment.
- Legal action and/or prosecution if deemed necessary.

Employees and students are required to sign the district's Acceptable Use Policy either in the schools' employee handbook, as a form provided by the technology department at the beginning of the year or as part of the district's Technology Handbook before Internet or network access shall be allowed. Users are also agreeing to the district's Acceptable Use Policy each time they click on the "OK" button on the AUP splash screen when logging into a district-owned device.

Stone County Schools

Employee Acceptable Use Policy Agreement

Name: (Print): _____
Position: _____
School / Department: _____
E-Mail Address: _____

I have read the district Acceptable Use Policy. I agree to follow the rules in this policy.

I understand that if I violate policy rules, I may be denied service, face disciplinary action and/or have computers and other technologies removed from my possession. I further agree to educate my students on the contents of this document and the consequences of failing to meet its requirements.

I hereby release the district, its personnel, and any institution with which it is affiliated, from any and all claims and damages of any nature arising from my use of or inability to use, the district's network, Internet and or any other technologies provided, including but not limited to, claims that may arise from the unauthorized use of the system to purchase products or services.

Signature:_____ Date: _____