Technology & User Agreement Handbook

Smith County School District (SCSD) provides the privilege of Internet access to district faculty, staff, students, and occasionally guests. Each user, as well as a minor's parent or guardian, voluntarily agrees to release, hold harmless, defend, and indemnify, the Smith 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, miss-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 can & will be restricted as required to comply with the Children's Internet Protection Act (CIPA). Web browsing may be monitored, and records are retained to ensure compliance.

Users are expected to respect the SCSD web filter and shall not attempt to circumvent the filter when browsing the Internet while using the SCSD network, either wired or wirelessly. 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 and have the head principal of the campus send to the Director of Technology for review.

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.

Smith County School District makes no warranty of any kind, either expressed or implied, regarding the quality, accuracy or validity of the data on the Internet.

SCSD NETWORK RULES

- *A. The person to whom an SCSD network account is issued is responsible at all times for its proper use.*
- *B. 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, detention, suspension, expulsion or other remedies applicable under the school disciplinary policy, and state or federal law.*
- *C. Any district employee who uses the SCSD network inappropriately is subject to disciplinary action, including dismissal.*
- *D. Under no conditions should a 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.*
- *E. 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.*
- *F. Users will immediately report to school district authorities any attempt by other network users to engage in inappropriate conversations or personal contact.*
- *G. Any non-standard software that is needed to perform a specific job function will need to be brought to the attention of the Technology Director. Those applications shall be the sole responsibility of that department 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)

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

- *H. Use school technologies for school-related activities.*
- *I. Follow the same guidelines for respectful, responsible behavior online that they are expected to follow offline.*
- *J. Treat school resources carefully and alert administrative staff if there is any problem with the technical operations of a device.*
- *K. Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.*
- *L. Alert a teacher, administrator, or other staff member if they see threatening, inappropriate, or harmful content (images, messages, and posts) online.*
- *M. Use District technologies at appropriate times, in approved places, for educational pursuits.*

UNACCEPTABLE USES OF THE TECHNOLOGY

(Not all *Inclusive)*

N. *Violating any state and/or federal law (i.e., copyright laws).*

O. *Using profanity, obscenity, or other language that may be offensive to others.*

P. *Making personal attacks on other people, organizations, religions, or ethnicities.*

Q. *Accessing, downloading, 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.)*

R. *Not respecting the privacy of a person by posting personal contact information, such as work/home address, telephone, email, photographs, or names, without obtaining prior permission from the person affected. Student information shall be posted only with written parent/guardian permission.*

S. *Forwarding personal communication without the author's prior consent. Using the Internet for commercial purposes, financial gain, personal business, producing advertisement, business service endorsement, or religious or political lobbying is prohibited.*

T. *Destroying or altering the files of another user or viewing or taking the files of another user.*

USE OF OUTSIDE EMAIL PROVIDERS & STIPULATIONS FOR USING DISTRICT EMAIL CLIENT AS DISTRICT REPRESENTATIVE

(Teachers, Administrators, Managers, etc.)

Use of "Internet mail" by students, staff, and faculty such as Yahoo mail, Gmail, and POP3 accounts provided by their "home" Internet service providers is NOT permitted. Beginning in the 2019-2020 school year, the District blocks the use of Internet mail accounts not managed by SCSD. All "OFFICIAL" communications, e.g., Teacher to Parent, Teacher to Student, Staff to Staff, must be via the district's e-mail system or at any given time an approved solution for such communications. This includes, but is not limited to, teachers who guide extracurricular activities such as Clubs, Choirs, Bands, Athletics, and the like.

FILTERING

An Internet filter is in place for Smith County School District. This filter is a critical component of the SCSD network as well as the federally required Children's Internet Protection Act (CIPA) compliance ruling since it allows valuable online Internet access while restricting access to specific unwanted material in the following categories:

Pornography, Gambling, Illegal Drugs, Online Merchandising, Hate Speech, Criminal Skills, Alternative Journals and Other Undesirable Materials.

The filter is updated daily 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 will be supervised at all times by a teacher while using the Internet. All Internet hits are logged and archived to include the date/time, IP address and account of the user of the workstation making the request.

Attempts to bypass the school 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, detention, suspension, expulsion, termination of employment or other remedies applicable under the school disciplinary policy, and state or federal law.

WORKSTATION MONITORING

All data transferred and/or transmitted over the SCSD network is monitored and recorded. All data transferred or transmitted over the network can be tracked and identified, and the originating user can be held liable if their use of the network/device 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 email, text documents, digital photographs, music, and other digital or electronic files. If a device continues to try to connect to an inappropriate site, that device will be remotely monitored and the individual using that workstation will be reported to District Administration.

TECHNOLOGIES COVERED

SCSD may provide the privilege of Internet access, desktop computers, mobile computers or devices, video conferencing 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.

Thus, 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 those released in the future, not just those specifically listed or currently available.

EMAIL

Employees and students SCSD email is the property of SCSD. SCSD archives all employee & student email. It is the responsibility of the employee and student to maintain this email account appropriately. When user email accounts are suspended due to the end user no longer being enrolled or employed by SCSD, the account will not be restored without the user making a person meeting with members of the IT Staff.

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 information about other employees or any student using email.

If users believe a computer or laptop they are using might be infected with a virus, they should alert the Technology Department. Users should not attempt to remove the virus themselves or download any programs to help remove the virus.

ONLINE ETIQUETTE

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

Users should remember not to post anything online that they would not want students, parents, teachers, or future colleges or employers to see. Once something is online, it cannot 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 appropriately cited, giving credit to the original author.

PERSONAL SAFETY

Users should never share personal information, including phone number, address, a Social Security Number, birthday, or financial information, over the Internet without a signed compliance form from a parent or guardian of any student. Users should recognize that communicating over the Internet brings anonymity, associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet in person someone they meet online without parental / guardian 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, parent if using the device at home).

CYBER BULLYING

Cyber bullying includes, but is not limited to, harassing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking, as such cyber bullying 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 described in SCSD Policy IJNDB-1 – Responsible Use of the Internet and Cyber Bullying. In some cases, cyber bullying can be a crime. Users should remember that online activities might be monitored.

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

LIMITATION OF LIABILITY

SCSD will not be responsible for damage or harm to persons, files, data, or hardware. While SCSD uses filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

SCSD will not be responsible or liable for, financially or otherwise, unauthorized transactions conducted over the SCSD network.

VIRTUAL MEETINGS

All virtual meetings hosted by any SCSD employee are monitored and recorded. Virtual meetings are an extension of the school the student attends and follows any rules or guidelines set by that school. The teacher reserves the right to limit the student’s ability to communicate or attend any school sanctioned virtual meeting.