# SACS Technology Acceptable Use Policy - 2014

## 1. Mission and Belief

The Metropolitan School District of Southwest Allen County ("SACS" or the "District") shall provide its students, faculty, and staff access to the Internet to promote educational excellence and to achieve the District's educational mission, goals, and objectives. Use of the Internet should be based on specific job and curriculum-driven objectives and goals.

SACS administration believes it is essential that students be provided with the proper 21st Century tool set that promotes student success now and in the future. In recent years, a multitude of new and exciting technological devices and applications have become available. The Internet and Web 2.0 allow collaboration, blogging, student construction, wikis, email, and personal productivity tools. Devices including cellular telephones, mini laptops, tablets, PDA's, and other mobile devices are making great inroads with our students. The school-wide network has the potential to provide and facilitate a learning experience beyond the classroom walls. All of these technologies, when properly used, will promote educational excellence while creating a true culture of learning by encouraging collaboration, communication, creativity, innovation, problem solving, research, inquiry, and productivity within the school day. Furthermore, these new technologies allow a rigor and relevance that will supersede the school walls allowing for learning opportunities that include the community, state, nation, and world, and providing students real-world learning experiences. These opportunities are essential for our students whose future includes a highly competitive high school, college, and workforce environment. With this in mind, all students must understand that the implementation of these new technologies makes it imperative that SACS provide a ***Technology Acceptable Use Policy***.

## 2. Why an AUP [Acceptable Use Policy]?

**a.** State and Federal technology funding requires such a policy if SACS provides Internet to staff, students, and other users.

**b.** Users must understand that illegal, unethical, inappropriate, and distasteful use of the technologies mentioned can have harmful consequences to the School and its stakeholders, including its students. The purpose of the AUP is to minimize the likelihood of any negative outcomes by educating students, staff, and parents while setting expectations and standards to protect SACS and its stakeholders.

## 3. Internet Use

**a.** Digital resources, information, and interaction are essential for the education of today's digital native. The intent of the SACS Technology AUP is to facilitate the learning of academics, citizenship, and social skills necessary to be successful in an ever-increasing digital environment.

**b.** The Internet enables users to explore thousands of libraries, databases, bulletin boards, and other resources. Use of the Internet is an integral part of the District's curricula. Faculty members will provide guidance and instruction about the Internet to students.

## 4. Responsibility of the MSD Southwest Allen County Technology User

**a. Objectionable Material:** Use of the Internet to access or process visual depictions of obscenity, child or adult pornography and/or materials harmful to minors, inappropriate text files, or files dangerous to the integrity of the network is prohibited. Do not access, compose, upload, download, or distribute pornographic, obscene, or sexually explicit material or language. Even with protections in place [see

SACS Filtering], as users use the Internet, it is possible, by accident or intent, they will see, receive, transmit or distribute objectionable material. Moreover, it is possible that improper exchanges between users, both within and outside the SACS network, may occur. Although SACS takes reasonable steps to prevent users from such experiences, it is impossible to eliminate all inappropriate material all of the time.

**b. Law Violation:** Internet use may not violate any local, state, or federal laws. Do not use the network to violate any other school policy. This includes, but is not limited to, transmission of copyrighted material, threatening, obscene, pornographic or sexually explicit material, or material protected by trade secret.

**c. Bypassing SACS Filtering:** Users are prohibited from bypassing or attempting to bypass SACS servers or Internet filters by any means, including, but not limited to, use of proxies or other anonymous website surfing.

**d. Internet is a Privilege:** Internet access is a privilege, not a right. With this in mind, access entails responsibility. As previously stated, users are required to use the Internet and District technology equipment for job or school-sponsored educational purposes only.

**e. Personal Use:**

i. Any use of the network for personal or commercial business is prohibited.

ii. Any use of the network for product advertisement or partisan political lobbying is prohibited.

iii. Users may not purchase goods or services through SACS network or SACS-assigned equipment for personal use. This further prohibits such use through SACS-assigned equipment used outside the physical boundaries of SACS, even if through a personal network.

**f. Proper Behavior:** Utilizing school-provided Internet and technology, users are responsible for proper behavior just as they are in a classroom or any other area of the school.

**g. Bully/Harassment**: Users shall not use the SACS network or SACS-assigned equipment to harass or bully others. This further prohibits such use through SACS-assigned equipment outside the physical boundaries of SACS, even if through a personal network.

**h. Identification/User Account:**

i. Do not log in under another user's username, or access another individual's files, information, or software without prior authorization from a SACS staff member.

ii. Keep all passwords secret and contact a staff member immediately if another person has learned a password.

iii. Do not vandalize, damage, or disable the files of others. In direct compliance with Child Internet Protection Act (*see* Section 7(b)), SACS attempts to provide privacy to all of its users.

iv. SACS users are also responsible for protecting their own and others’ identities. This includes, but is not limited to, the following items: each user will not post or submit their name, personal identifying information, address, location, identification or telephone numbers, or any of the previously mentioned categories of information relating to other users. This includes submitting such information to or through websites blogs, wikis, chats, glogs, forums, email, or any other curricular or non-curricular locations on the network or Internet.

NOTE: This restriction does not apply to student use of SACS-approved sites and/or employee use of sites related to legitimate job or academic purposes. For instance, classes may use SACS-approved Web 2.0 applications such as, but not limited to, MyBigCampus and Google Docs, which serve as an exception to this provision. Such Web 2.0 tools will only be used after proper approval and permission has been secured and in accordance with all policies, procedures, and guidelines applicable to them. And, even when proper approval and permission has been secured, users must still take reasonable steps to ensure safety, security, and privacy for all stakeholders. The narrow exception for "other legitimate academic purposes" is meant to allow students to submit information to apply for college, register for the SAT, apply for employment, and other closely related activities. If in doubt, students will check with their teacher and/or the SACS AUP before submitting any of the information described above. Likewise, employees will check with their supervisor.

**i. Digital Citizenship:** Electronic and/or digital communications should be tasteful and school-appropriate. All communication should be polite. Remember that one is communicating with other human beings whose culture, language, and humor have different points of reference from your own. Never forward others information without their knowledge and approval. Understand when it is proper to use text messaging jargon.

## 5. Other Guidelines

**a. External Storage Devices:** Any external storage device (flash/thumb drives, memory cards, external hard drives, CDs/DVDs, etc.) must be checked for viruses before use.

**b. Downloading, Software Installation:** Downloading or installing software is not permitted without authorization from the SACS CMT [Community Media Technology Department]. Adobe software (Acrobat Reader, Flash, etc.), Java, and other common and widely-used software required to use the Internet is permissible. Before downloading any software, the user must meet the following criteria:

i. Receive authorization to install the software;

ii. Verify it is legal to install or download the software under copyright laws;

iii. Ensure that the software is virus-free; and

iv. Ensure that the software meets license requirements of its software vendor.

**c. Personal Devices:** The following applies to the use of personal devices while within the physical boundaries of SACS. Personal devices are used and brought to class only with teacher permission and used only for educational purposes, or for school-related activities (e.g., extracurricular activities). They must be turned off when entering and exiting the classroom. If permission is granted to be turned on, all use is directed toward class work, and only school network connections are permitted. Users are responsible for their personal property, and the school assumes no liability for student property. Users must adhere to the SACS AUP regarding the use of personal electronic and/or mobile devices. School administration and/or teacher(s) will provide parameters for this use. *NOTE: Text messaging, email, voice over IP, chat rooms and instant messaging, regardless of device or network ID, used inappropriately may be deemed offensive or disruptive to the educational process, resulting in disciplinary action.* Employees may not bring or use personal electronic devices that use SACS network without prior approval from their supervisor and SACS CMT [Community Media Technology Department].

**d. Personal Devices Attached to SACS Hardware:** Personal Devices attached to SACS devices are not permitted unless otherwise noted.

**e. Copyright/Intellectual Property:** All users will follow copyright procedures. All resources obtained/used should be properly cited. All users are expected to respect the rights and intellectual property of others in accordance with Federal Copyright Law and Fair Use Policy, which includes multimedia owned by a user or downloaded at home. If a user is granted permission to post on the web, it will comply with the SACS AUP and other applicable policies.

**f. Appropriate Behavior:** No user shall use SACS technology or personal devices in any manner which could be deemed offensive or disruptive to the educational process or job requirements. Inappropriate behavior includes, but is not limited to, communication, documents, or any other tangible means of expression, that contain sexual implications, racial slurs, gender-specific comments, or any other statement that offensively addresses a person's age, sexual orientation, religious or political beliefs, national origin or disability. Inappropriate behavior also includes searching, contributing, downloading, and/or viewing inappropriate material, threatening individuals or organizations, disrupting and damaging District property/ networks, or digital cheating.

**g. Log In And Password Etiquette:** Each user has been given a login and password for various school resources. A user shall neither share his/her login and password nor use another user's login and password to gain access to and fraudulently use another's account. Users will not seek to gain access to another user's accounts by any means including, but not limited to, looking through others' materials or by watching another user log in. *NOTE: To protect your privacy always log on and off each machine you use at school and in other public locations. Never accept a browser's request to remember your login information.*

**h. Email, Text Message, Posts, and Chats:** Such services, if available and necessary for curricular or job facilitation, will have access provided by SACS. Such access does not imply permission of use unless integrated within the classroom learning environment. In these cases, students and other users will be directed to use specific resources and will be expected to abide by regulations provided in the SACS AUP and the SACS 1 To 1 Laptop Initiative Guidelines. This includes all aspects of proper Digital Citizenship defined in these documents.

**i. Vandalism:** Vandalism includes, but is not limited to, defacing, disassembling, or destroying any part of the computer hardware, software, or settings. Users are not to move any cables, switches, and plugs associated with the computers or network. Vandalism also includes any attempt to steal or damage data of another user, the SACS network, the Internet, or any other connected agency or network. The offender may be required to pay for the repair or replacement of damaged hardware, or for services needed to undo software changes.

**j. 1 To 1 Laptop Initiative:** Students are expected to abide to all mandates stipulated in this SACS AUP, regardless of the location of the school-owned laptop/equipment. This includes expectations and requirements for the 1 To 1 Laptop Initiative. It is important to read the policy stipulated in the 1 To 1 Laptop Initiative Guidelines.

## 6. Loss of Privilege

Any violation of SACS AUP may result in loss of District-provided access to the school technology equipment and the Internet. Additional disciplinary action may be applied at the building level in keeping with existing procedures and practices regarding inappropriate behavior. Where applicable, law enforcement agencies may be involved.

## 7. SACS Responsibilities

**a.** The District’s responsibilities include establishing reasonable boundaries of acceptable use, educating students and parents about acceptable use, providing general supervision, and enforcing acceptable use guidelines. The District assumes no responsibility for any costs, liabilities, or damages that a user may incur while accessing the Internet.

**b. CIPA** [Child Internet Protection Act]: SACS will comply with the rules of CIPA. CIPA requires schools using E-rate discounts to operate *"a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to inappropriate resources and websites that could be harmful to minors."* Such a technology protection measure must be employed during any use of such computers by minors.

**c. SACS Filtering:** The District makes reasonable efforts to filter access to the Internet to prevent, for example, access by both adults and minors to visual depictions that are obscene, child pornography or, with respect to use of the computers by minors, harmful to minors.

**d. SACS Monitoring:** SACS-monitored direct electronic communications are not private. These include, but are not limited to, blogs, wikis, forums, email, instant messaging, broadcasting and video/audio conferencing. Their use must be curriculum-related and reflect all guidelines herein with particular emphasis on protection of personal identification information. Files stored on or transmitted through school-based computers, devices, SACS networks, or other cloud-based services will be monitored. This includes keystrokes entered into any site. SACS reserves and intends to exercise the right to review, analyze, edit or otherwise supervise all use of the Internet while also regulating use by students.

**e. Student Education:** In accordance with the school’s legal obligations, students shall receive education regarding, but not limited to, the following: (1) appropriate online behavior in social networking sites, chat rooms, electronic communications, etc; (2) the dangers inherent with the online disclosure of personally identifiable information; and, (3) consequences of unlawful activities, including cyber-bullying awareness and response, and other unlawful or inappropriate online activities by students, such as hacking.

**f. DISCLAIMER:** SACS, its employees and agents, make no warranties of any kind, neither express nor implied, concerning the network and Internet access it is providing. Also, SACS is not responsible for any disruption of network services or the loss of content that resides on the school machines, network, cloud based services, or related infrastructure. It is always wise to make backups of all work. Furthermore, SACS is not responsible for:

i. The accuracy, nature, quality, or privacy of information stored on any storage device, hard drives or servers, or of information gathered through the Internet access;

ii. Any damages suffered by a user, including, but not limited to, loss of data resulting from delays or interruptions in service, computer viruses, or to personal property used to access computers, networks, or the Internet; or

iii. Unauthorized financial obligations resulting from the use of the network or Internet.

### 8. Opt Out

Parents or legal guardians not wishing their student to have Internet access for curricular use must notify the school’s administrator in writing.

## 9. Policy Understanding

It is important that students, staff and parents understand this policy. Violation of these guidelines can result in the termination of a user’s access to SACS network. In addition, staff may be subject to disciplinary action, up to and including dismissal from employment