COMPUTER NETWORK AND INTERNET USE POLICIES

The goal of the SAS Technology Department is to help create a mission-appropriate teaching and learning environment which includes safe and secure technology use. It is the policy of SAS to comply with the Children's Internet Protection Act [Pub.L.No.106-554 and 47USC 254(h)]

In support of the goals of acceptable Internet use outlined by the U.S. Dept of Education, SAS encourages and educates students on the responsible use of computers and web-based technologies.

It is the policy of SAS to keep staff and students safe and to maintain an environment that promotes ethical and responsible conduct in all online network activities.

It is the policy of SAS to prevent user access to, or transmission of, inappropriate material over its network.

It is the policy of SAS to prevent unauthorized access to online information.

It is the policy of SAS to prevent unauthorized online disclosure, use, or dissemination of personal identification information.

ACCEPTABLE and APPROPRIATE USES of SAS TECHNOLOGY

SAS provides its users a G Suite for Education (Google Applications) account, which includes email, drive, sites, calendars and other features. It is strongly encouraged that students do not use their SAS email for personal use and keep it for school use only.

If requested, users will be provided with a Microsoft Office 365 account, which includes Word, Powerpoint, Excel, and other applications.

All users will be provided a community SSID (network logon) and password specifically designated according to his/her relationship with the SAS community. (SAS_Students for student use; SAS_Faculty for faculty use; SAS_Guest for all guests.)

In addition to network access and G Suite for Education accounts, users will also be given a username and password to log in to the BlackBaud Portal. This is where student users can see schedules, grades, comments, assignments, and other important information.

Wireless internet access is available to all individuals with a SAS email account.

Wired network access is strictly prohibited for all students unless implicitly authorized by the Technology Department. Boarding students are allowed wired internet access in the residential houses ONLY.

Users are responsible for and strongly encouraged to back up school work and other personal data on their computers through a thumb drive or an external hard drive. It is recommended that users utilize Google Docs for the creation and storage of school related documents. This will enable users to access their files from any Internet enabled computer and easily share their work with others, and will remove the need for keeping backup documents. SAS owned devices utilize Google Drive FileStream as an additional cloud based backup.

All users, including students, should check their email at least twice a day. SAS uses its email system to disseminate important community and personal messages as well as homework assignments and other school related work.

SAS subscribes to a managed web filter. This filter was not created by SAS; there may be some websites that are appropriate which are blocked, and some inappropriate content that is not blocked. Faculty are encouraged to open a trouble ticket with requests to unblock sites suitable for educational purposes. All student requests to unblock a site must be approved by a faculty member.

UNACCEPTABLE USES of SAS TECHNOLOGY

Dishonest or deceitful behavior -- including any attempt to accuse, use, or harm other users' account or date.
Violation of confidentiality -- including unauthorized communication of another person's personal information, such as name, address, phone number, credit card numbers, passwords, etc.
Intentional use of invasive software such as viruses, worms, or other detrimental activities.
Trespassing in another user's folders, email, or work files. Using, or attempting to use, another person's account and password to access information on the network is considered a violation of the Honor Code.
Hacking, Flooding, Sniffing Network, Cracking and Spoofing--this includes using someone else's user-name and password to gain access to email, voicemail, or other stored information. Users may not use passwords or access codes which prevent access by the System Administrator. Users are prohibited from "hacking" into other systems or "cracking" other passwords or access codes. No electronic communication may be created, transmitted or stored which attempts to hide the true identity of the creator or sender "spoofing". Users are strictly prohibited from flooding the network or other networks over the internet.
Vandalism -- including any attempt to harm or alter the functioning of the network, attempts to bypass restrictions, deliberate abuse or destruction of computer equipment, destruction of data or misuse of the network resources, telephones, fax/copy machines, voice-mail system, computers, network hardware, wiring or wireless devices. At no time should there be food, candy, or drinks in any of the SAS computer areas, including the Tech Lab, Agee Library, Film Classroom, StorySpace, or Recording Studio.
Harassment, Cyber Bullying, Sexting--including threatening, abusive, or sexually explicit language, profanity, vulgarity, obscenity or other language or images which are offensive or degrading to others. (See Cyber Bullying and Harassment under Safety and Security)
Pornography -- including viewing, storing or transferring obscene, sexually explicit or pornographic materials.
Inappropriate Content--viewing, storing, or transferring materials promoting drugs, alcohol, tobacco, or other illegal activity are all unacceptable uses of technology. Images which are considered "gore" or show violence or death are also considered by SAS to be inappropriate to view or show others. Legitimate news sources are an exception.
Plagiarism--This includes using, writing or images created by another person without proper citation or permission; transferring, utilizing, or storing material in violation of copyright laws or license agreements; and intentionally infringing upon the intellectual property rights of others.
Profit and Promotion -- including use of the SAS network or internet-based resources for solicitations, advertisements, or promotions (whether charitable, political, religious or other) for any purpose that is not an official SAS endeavor.
Flaming -- which includes sending or posting content that contains offensive material directed at others or negatively represents SAS.

ONLINE INSTRUCTION EXPECTATIONS

Students using video conferencing platforms (i.e. Zoom or Google Meet) for on-campus or off, should follow the etiquette guidelines provides by each instructor and also:
Use (@sasweb.org) school accounts to log in to the designated video conferencing platforms.
Turn on the video feed during the session. Students must ask for video exceptions from the instructor.
Use and display their first and last names that are recognized by SAS for the whole session.
Never share meeting login info with anyone else.
Never capture, record, or distribute images or videos of the video conferencing classroom without teacher permission..

CYBER CITIZENSHIP
Use of the school's computer network is a privilege, not a right. As a member of the SAS school community, you are responsible for adhering to the policies outlined in the document, regardless of whether you use our school network, a cell phone, iPod or iPad, 3G or LTE network connection or any other internet connection.
Use of the internet should be limited to academic pursuits during school hours and evening during study periods.
Users accessing the SAS network, the internet, email or other messaging programs (IM chat, blogging, texting, etc.) are considered to be representatives of SAS school at all times and should behave appropriately.
If you are on a community computer and find an account that is still logged in, be considerate and log out that person. Do not look at others' email or files, as this would be considered trespassing and is an invasion of privacy.
Cyber Bullying and Harassment--SAS School endeavors to provide a safe, positive learning environment for everyone. It is our policy to maintain an educational environment in which cyber bullying and harassment in any form is not tolerated. Each person at SAS shall be responsible for respecting the rights of his/her fellow community members and help to ensure an atmosphere free from all forms of cyber bullying and harassment.
Cyber Bullying is the use of the internet, cell phones or other devices to send, post or share text or images intended to hurt, embarrass or intimidate another person.
Cyber Harassment is repeatedly sending hurtful, embarrassing and intimidating messages.
Any member of the community who engages in cyberbullying or harassment in violation of this policy may be subject to disciplinary response up to and including suspension, expulsion or termination.
Anyone who has been cyber bullied or harassed shall immediately report the incident to the Head of School, an administrator or the Dean of Students. Do not delete any evidence that can be used to investigate an incident.
Complaints of cyber bullying or harassment shall be investigated promptly, and corrective action shall be taken when a complaint is verified.

PRIVACY AND SAFETY
The SAS Technology Department has the right to and does monitor all uses of technology. Web connections are logged and filtered. Users cannot expect privacy rights to extend to the use of school-owned equipment. Users have individual passwords for their G Suite for Education,

BlackBaud, and other resources that utilize the network. However, communications created, stored, sent or retrieved on such systems are not confidential, as these systems are accessible at all times by the school.

SAS reserves the right to review, audit, intercept, monitor, access, print and disclose all messages created, received, stored or sent using the school's information and communication systems.

Users may be required to disclose their password to the Network Administrator.

For your safety, you should not share personal information such as your full name, address, telephone number, social security number, or other information to unknown individuals which may lead them to you or use your information.