……

Attalla City Schools
Character.Commitment.Community.

101 Case Avenue SE | Attalla, AL 35954
P: 256-538-8051 | F: 256-538-8388

INTERNET AND TECHNOLOGY USAGE

The Children's Internet Protection Act (CIPA) requires schools who receive federal technology funds to have certain policies in place.

> *"Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them." - http://transition.fcc.gov/cgb/consumerfacts/cipa.html*

In compliance with CIPA requirements, Attalla City Schools (ACS) has adopted this Technology and Internet Use and Safety Policy. This policy is the rules and guidelines under which all members of ACS (students, faculty, and staff) will be held accountable.

ACS believes that the information available from electronic sources alters the educational environment by opening virtually unlimited resources. We strive to provide faculty, staff, and students with appropriate technological resources to support a rich educational experience. In order to provide these resources, ACS will take precautions to ensure reliable communications and restrict access to inappropriate information or materials. However, given the global nature of the internet, it is impossible to control and limit all materials. We believe the value of the information and interaction available via the internet far outweighs the possibility that users may procure material that is not consistent with the educational goals of the system.

USAGE GUIDELINE

ACS provides students and staff access to various electronic resources including a wide range of educational materials through Internet and computer online services. ACS uses content filtering technology in compliance with the CIPA on all system owned computers or networks with Internet access to protect against unacceptable web content. However, no web filtering technology is 100% effective. ACS realizes this fact and reserves the right to monitor online activity using any of a variety of tools.

Student and Staff Safety – Do not send or post any message or information that includes personal information such as: home address, personal phone numbers and/or last name for yourself or any other person. Likewise, ACS staff is not permitted to post this information to public domains (i.e. class web page or Internet). Student likenesses (either pictures or video) and/or work may be posted on district/school/classroom websites without identifying captions (such as full names). No likeness and/or work should be posted to public or private web sites that are not owned or sanctioned by ACS.

Extended Safety K-5 – Teachers of students in grades K-2 will access appropriate websites for their students. Students in grades 3-5 may not attempt to access any Internet resource without the prior consent of the teacher.

Usernames and Password Protection – Internet, e-mail, and computer usernames and passwords may be provided and are for each individual's personal use only and are, therefore, confidential. Never share your password nor use another person's password. If you suspect that someone has discovered your password, you should change it immediately and notify your teacher or administrator who in turn will notify the technology director. As words and phrases are easily hacked, when establishing a password one should keep in mind that strong passwords consist of a combination of at least eight upper and lowercase letters, numbers, and symbols. ACS will establish minimum requirements for strong passwords.

The individual to which a username is assigned is responsible for ALL technology use which is associated with that username. For that reason, a compromised account should be reported immediately.

Privacy – Email is no more private than a postcard. Students and staff need to know that files stored on school computers are not private. Network and Internet access is provided as a tool for educational purposes only. The District has the right to monitor, inspect, copy, review, archive, and store at any time and without prior notice any and all usage of the computers, network, Internet access, and other electronic communications including transmitted and received information. All information files are the property of the District and no user shall have any expectation of privacy regarding such files. However, no user has the right to access another user's files with the exception of district technology staff or the superintendent's other assigned agent.

Online Etiquette – Follow the guidelines of accepted behaviors within the school handbook. Use appropriate language and graphics. Swearing, vulgarities, suggestive, obscene, belligerent, harassing, threatening or abusive language of any kind is not acceptable. Do not use school online access to make, distribute, or redistribute jokes, stories, cyber bullying, obscene material or material which is based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation. No user should use the system's access for any activity that produces personal gain.

Messaging – E-mail addresses may be provided to students, teachers, and staff. Teachers may incorporate: email, blogs, podcasts, video conferencing, online collaborations, instant messaging, texting, Virtual Learning Environments and other forms of direct electronic communications (i.e. cell phones, cameras) or web tools applications for educational purposes. Although teachers monitor student online activity, it is the direct responsibility of the user to comply with this acceptable use policy.

Blogging/Podcasting/Learning Management – The use of blogs, podcasts, Learning Management Systems, or other web tools are considered an extension of the classroom. Whether at home or in school, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, Learning Management Systems, or other web tools. Students using blogs, podcasts, Learning Management Systems, or other web tools are expected to act safely by keeping ALL personal information out of their posts. Comments made on school related blogs should follow the rules of online etiquette detailed above and will be monitored by school personnel. If inappropriate, they will be deleted. Never link to websites from a blog without reading the entire article, including its advertisements, to make sure it is appropriate for a school setting.

Plagiarism/Copyright/Licensing – Plagiarism is the act of using someone else's words or ideas as your own. Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text. Plagiarism of Internet resources will be treated in the same manner as any other incidences of plagiarism, as stated in the school handbook. In addition, all students and faculty must adhere to the copyright laws of the United States (P.L. 94-553) and the Congressional Guidelines that delineate it regarding software, authorship, and copying information. All students and faculty should also adhere to the Creative Commons licenses where the author/artist denotes what media may be shared, remixed, or reused.

Proxies – The use of anonymous proxies or any other technology designed to circumvent content filtering is strictly prohibited and is a direct violation of this agreement.

Illegal Activities – Use of the network for any illegal activities is prohibited. Illegal activities include, but are not limited to: (a) tampering with computer hardware or software, (b) software piracy (c) unauthorized entry into computers and files (hacking), (d) knowledgeable vandalism or destruction of equipment, (e) denial of service or other electronic attacks (f) deletion of computer files belonging to someone other than oneself, (g) uploading or creating of computer viruses, (h) distribution of obscene or pornographic materials, and (i) sexting. Such activity is considered a crime under state and federal law. Users must be aware that any illegal action carried out over the Internet will be reported to law enforcement officials for possible prosecution. Please be advised, it is a federal offense (felony) to break into any security system. Financial and legal consequences of such actions are the responsibility of the user (staff, volunteer, and student) and student's parent or guardian.

District Property – All school owned computer and network equipment is the property of Attalla City Schools and is subject to this agreement. Modification of district owned equipment is strictly prohibited without the consent of the district Technology Coordinator. Modification includes, but is not limited to, installation of software or operating systems, replacing or changing hardware, changing configurations, or attempting to circumvent any security devices. Modification or damage to such systems could be deemed an illegal activity and subject to the actions listed elsewhere in this agreement.

Personal Property – Any personally owned device (including but not limited to computers, cell phones, tablets, etc.) that is used to access the ACS computer network or circumvent its security measures may be subject to search and seizure for the purpose of investigating activity that is believed to be in violation of this agreement.

Operational Efficiency – It is the intent of the ACS Technology Department to maintain an efficient and reliable computer network in order to provide learning opportunities to all ACS students. Therefore, any activity that limits or adversely affects the operations of the computer systems or networks will not be permitted. ACS may control, limit, or deny activities that are deemed to reduce efficiency, whether they be malicious or not.

Training – ACS will have resources available for Teachers, Staff, Administrators, Students, Parents, and Guardians for the purpose of educating the legal, ethical, and safety practice of software and hardware usage. These resources may be utilized as part of a formal training or may be available as a self service resource.

Removable Media and Network Storage – Media such as writable Compact Disks or USB drives are permitted as it pertains to an accepted educational purpose. Such media is subject to the Personal Property clause above, and is subject to automatic search by district antivirus or other security software. Files containing malicious code may be cleaned or deleted without the user's permission. Access may be blocked to files deemed unacceptable by the Technology Department. Network storage may be made available to faculty, staff, and students for valid purposes. This storage space may be limited or controlled as required by the Technology Department to ensure equitable and efficient use of limited technology resources.

TERMS OF AGREEMENT

Attalla City Schools reserves the right to deny, revoke, or suspend specific user privileges and/or to take other disciplinary action, up to and including suspension, expulsion (students), or dismissal (staff) for violations of these Guidelines. Users and/or their legal guardians may also be held financially responsible for damages associated with violations of this agreement. The District will advise appropriate law enforcement agencies of illegal activities conducted through the ACS Internet Connection. The District also will cooperate fully with local, state, and/or federal officials in any investigation related to any illegal activities conducted through the service. The school district and its representatives are not responsible for the actions of the users or the information they access.

Individuals are expected to report any violations of this policy and/or problems with the security of any technology resources to the Principal, School Technology Planning Committee, or Technology Department. Failure to do so could constitute a violation of this policy and is subject to the consequences listed above.

Any questions about this policy, its interpretation, or specific circumstances shall be directed to the System-Wide Technology Coordinator.

Attalla City Schools
Character.Commitment.Community.

101 Case Avenue SE | Attalla, AL 35954
P: 256-538-8051 | F: 256-538-8388

STUDENT TECHNOLOGY RESOURCES AGREEMENT 2022-2023

STUDENT NAME: ____

SCHOOL: ____

I understand that Internet access is provided for educational purposes. I understand that Attalla City Schools will take precautions to eliminate controversial material as outlined in the Internet and Technology Use Policy. However, I also recognize it is impossible to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network. I understand that as a network user, I am responsible for my actions and that I am responsible for acting considerately and appropriately, in accordance with the Internet and Technology Use Policy.

I understand that by signing below, I agree to all conditions of the Internet and Technology Use Policy. I understand that I have no expectation of privacy, as defined in the policy, while using Attalla City Schools computers or network, and that my likeness (without identifying information) and/or classwork may be published to the school system or other sanctioned websites.

I understand that any or all of the following sanctions could be imposed if I violate any of the policies and procedures regarding the use of Attalla City Schools Technology Resources including the Internet.

1. Loss of access.
2. Additional disciplinary action to be determined at the individual school in line with existing practices regarding inappropriate language or behavior.
3. Financial Liability.
4. Legal action.

PARENT NAME: ____

PARENT SIGNATURE: ____

STUDENT SIGNATURE: ____

DATE: ____

Attalla City Schools
Character.Commitment.Community.

101 Case Avenue SE | Attalla, AL 35954
P: 256-538-8051 | F: 256-538-8388

FACULTY/STAFF TECHNOLOGY RESOURCES AGREEMENT 2022-2023

I understand that Internet access is provided for educational purposes. I understand that Attalla City Schools will take precautions to eliminate controversial material as outlined in the Internet and Technology Use Policy. However, I also recognize it is impossible to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network. I understand that as a network user, I am responsible for my actions and that I am responsible for acting considerately and appropriately, in accordance with the Internet and Technology Use Policy.

I understand that by signing below, I agree to all conditions of the Internet and Technology Use Policy. I understand that I have no expectation of privacy while using Attalla City Schools computers or network. I understand that private student information cannot be published to any publicly accessible source. I understand that student likenesses and work may only be posted to school system or other sanctioned websites, and any such posts cannot contain information to directly identify the students (such as full names).

I understand that any or all of the following sanctions could be imposed if I violate any of the policies and procedures regarding the use of Attalla City Schools Technology Resources including the Internet.

1. Loss of access.
2. Additional disciplinary action to be determined by the Board of Education in line with existing practices regarding inappropriate language or behavior.
3. Financial Liability.
4. Legal action.

FACULTY/STAFF NAME: ____

FACULTY/STAFF SIGNATURE: ____

DATE: ____