



Student Technology Handbook 2023-2024

Senatobia Municipal School District

www.senatobiaschools.com
Phone: (662) 562-4897
Fax: (662) 562-4996

104 McKie Street
Senatobia, MS 38668

TABLE OF CONTENTS

SENATOBIA MUNICIPAL SCHOOL DISTRICT 1:1 STUDENT DEVICE PROGRAM	3
RECEIVING A DEVICE	4
RETURNING A DEVICE	4
TAKING CARE OF A DEVICE	4
USING THE DEVICE AT SCHOOL	5
MANAGING AND SAVING DIGITAL WORK	6
OPERATING SYSTEM ON A DEVICE	6
RESPONSIBLE USE	7
PROTECTING AND STORING THE DEVICE	9
REPAIRING/REPLACING THE DEVICE	9
DEVICE TECHNICAL SUPPORT	10
CHROMEBOOK FAQs	10
TECHNOLOGY ACCEPTABLE USE POLICY	12
INTERNET SAFETY AND CYBERBULLYING POLICY	18
TECHNOLOGY AGREEMENT	19

Senatobia Municipal School District

1:1 Student Device Program

2023-2024

The mission of Senatobia Municipal School District's (SMSD) one-to-one (1:1) program is to create a prosperous, accessible, fair, and collaborative learning environment for each student and staff member. Only that type of environment will support the needed engagement and growth that will promote the transformative use of technology in regard of self-directed learning for all involved parties.

The eventual goal is to evolve students from passive learners to active scholars that are able to consume knowledge and grow to their full potential over their lifetime.

SMSD will create a learning community based on development for teachers to aid their creation of a baseline of high-quality instruction that embeds assessment and learning within; this will transform the teacher from a director to facilitator of learning, making the instructor a willing participant in the student quest for understanding.

The SMSD school board, district staff, and Senatobia community are valued members in the development of the student experience.

Device Purpose

Every student will be issued a student device; however, the district maintains ownership of the device throughout the student's possession of the device.

The device's sole function will be to provide each student with access to educational materials needed for collaboration with teachers and peers. The device is under no circumstances to be used for online gaming, social media, or any other non-educational uses.

The device will allow student access to online materials which are included but not limited to Google Classroom, Renaissance Place, and other ever-changing learning software purchased by the district.

Receiving a Student Device

District-Owned and Issued Student Device

- Devices will be issued during student registration at the beginning of the school year. Before a student is allowed a device, parents/guardians must sign and return the SMSD Student Device Agreement.
- Devices may be taken back up at the end of each school year at the discretion of school administration. Students will use the same device upon returning for the next school year and while enrolled in the district unless it is permanently or temporarily replaced due to maintenance, malfunction, or upgrade.
- There will be a damaged device fee of \$25 per each instance of damage.

Probationary Student Privileges

Probationary students may be required to turn their device in to their teacher at the end of the day for two weeks unless otherwise specified in the Acceptable Use Policy (AUP) or as deemed necessary by administrative staff due to outstanding circumstances or need.

Probationary Students are the following:

- New students to the district that weren't enrolled during the previous semester
- Students with poor attendance records, more specifically, students who have ten absences in three or more class periods during the present or previous semester
- Students who have violated the AUP during the current or previous semester

Returning a Student Device

- Students transferring from or graduating SMSD must return their issued device to the designated responsible support person at the attending school.
- Student devices that aren't returned will be considered stolen property; law enforcement agencies will be notified.

Taking Care of a Device

Students are responsible for taking care of the device they've been issued by the district. Devices with technical issues or need of repair should be reported to the student's teacher or administrator so they can submit a helpdesk ticket. **Do not take devices owned by the district to outside computer repair shops for any reason, regardless of accidental damage. Always allow in-house district staff to repair the equipment.**

General Precautions

- No food or drink around the device at any time.
- Insert all cables, plugs, and storage devices carefully lest they snap off and damage the device.
- Don't transport the device with anything plugged into it.
- Don't store the device in a bag while it's powered on. Always close the lid first.
- Never carry a device while it's open; shut the lid and then transport the device.

- Do not draw, write, or put any type of sticker on the device. Only a label with the student's name may be placed on the device. Stickers may be placed on the case.
- Do not cover the vents else the device will overheat.
- SMSD devices will have a device inventory tag on them at all times, and this tag must not be removed or altered. The purposeful removal or damage of the tag will result in disciplinary action. If the tag is accidentally damaged, no disciplinary action will occur. In that case, notify the teacher so that another tag can be issued in its place.
- Don't leave the device in a car or unattended in any public place.
- Devices must be fully charged every single school day; students are responsible for this. We ask that students charge them in the evening to be ready for the next day.
- If the device needs repair, report the need to a teacher or administrator so technology staff can be notified via helpdesk ticket.
- The student's barcode will be placed on the device with the inventory sticker to be used for identification purposes.

Transporting Student Devices

Screens are by far the most easily damaged part of a student device. Excessive pressure can cause warping and even cracking to the point that it can't be used until repair.

- Don't lean on the device while it's closed.
- Don't store the device while it's open. Always make sure the device's lid is closed for storage.
- Don't put anything heavy on top of the device as it could put pressure on the screen and break it.
- Don't use anything to poke, mark, or scratch the surface of the screen. (IE: Pencils, pens, etc.)
- Don't place anything on the keyboard of a device before closing the lid. (IE: Pencils, pens, thumb drives, etc.)
- Clean the screen with a soft microfiber or anti-static cloth.
- Use care with disinfecting and only use chemicals that are marked as safe for computer screens. Some may damage the screens and make them fade. Never spray liquid onto the device; alcohol applied to a cloth is enough for disinfecting both screens and keyboards.

Using a Student Device at School

Devices Left at Home

- If the parent/guardian is unable to bring the device to school, the student will have a chance to use a loaner device if there is one available.
- **Repeat violations will result in the loss of take home privileges.**

Devices Under Repair

- A spare device will be issued to students while their main device is being repaired.
- The spare device will be the student's responsibility. Any damages while the device is in the student's possession will be paid for by the student and/or their parent/guardian. Lost or stolen devices in the student's care, loaner or not, will result in the student and/or their parent/guardian paying the full replacement cost.

Charging a device

- Devices must be fully charged before the student arrives at school.
- Students are responsible for charging their device each evening in preparation for school the next day.
- **Repeat violations will result in loss of take-home privileges.**

Backgrounds

- Guns, weapons, pornography, inappropriate language, alcohol, drugs, and gang-related symbols or pictures will not be used as a screensaver or background. Use of this type of material will result in disciplinary action. Appropriate nature of the situation is to be assessed by school or district administration.

Sound

- Audio must be muted at all times except when the student has teacher permission.
- Headphones or earbuds may be used with teacher permission.

Account Access

- Students are responsible for their account. They must take care to protect their account password and should not lend it out to anyone. The account is the student's digital face and the only way to ensure the identity of the person turning in work.
- Any student that gives out their account information to another student **or** logs into another student's account is in violation of the AUP and subject to disciplinary action.

Managing and Saving Digital Work with a Student Device

- Google Workspace for Education is a suite of products similar to Microsoft Office. However it has capabilities such as mail, a shareable calendar, and access to Google Classroom to collaborate with peers and complete online classwork while storing it all in the Cloud so it won't get lost in the event of device failure.
- Users can access their documents anytime, anywhere, and on any device with an Internet connection.
- If Internet access isn't possible, and this is anticipated, documents can be put into 'available offline' mode for access until the device has Internet access again.
- Documents are stored online with Google Drive and are accessible with the student's login credentials.
- Before a student leaves the district, including before they graduate, those who want to save any of their work need to use Google Takeout to transfer them to a personal Gmail account. Graduating seniors will have until July 1 of their graduating year to transfer all needed data, but afterward the non-attending accounts will be deleted.

Operating System on a Student Device

- Managed student devices automatically update when needed, ensuring the device has the most recent version of their operating system without the user needing to do anything but restart when prompted.
- Managed student devices are built with layers of protection against malware, viruses, and security attacks, but users should still take care when clicking on suspicious or unexpected attachments or links.

Responsible Use

Responsible use guidelines apply to all district equipment, Internet, media, and communication. The guidelines will be adhered to by all students, faculty, staff, and administration.

General Guidelines

- Student devices are in compliance with the Children's Internet Protection Act (CIPA).
- Student issued devices will not be used to obtain or view things that are deemed inappropriate by CIPA. This includes but isn't limited to things such as pornography or other things considered obscene or harmful to minors.
 - It's against state and federal law to display any kind of sexually explicit image or document on any SMSD system.
 - Possession of explicit pictures and video of minors and/or the electronic transmission of explicit pictures and video of minors is a federal offense. Authorities will be immediately notified if district staff becomes aware of the possession or transmission of any such material.
 - Sexually explicit material may not be archived, stored, distributed, edited, or recorded using the district network or any district-owned resources.
- Students will have access to a wide variety of electronic media and communication that supports learning and research based on educational goals set by the district.
 - SMSD reserves the right to block any sites that are deemed objectionable or inappropriate to district staff.
- Students are responsible for their own ethical use of district resources provided for learning.
- Access to district technology and district-provided Internet is a privilege and not a right. Every employee, student, and/or parent is required to follow the rules of the AUP.
- Transmission of material in violation of federal or state law is prohibited. This includes but isn't limited to confidential information, copyrighted material, threatening or obscene material, and malicious software such as viruses or malware.
- Any attempt to tamper with the configuration of a device, the data on any of the servers, or the files of another user without consent of that user (consent such as a collaborative project in the scope of classwork and all things similar) will be considered vandalism and will result in disciplinary action in accordance with the handbook and applicable district policies.
- No student or staff can use the SMSD network or devices to spread a virus, worm, Trojan, trapdoor program, or other app that would be used maliciously to gain access or damage another user's system.
- Every user using the SMSD network should identify themselves honestly, accurately, and completely when setting up accounts on outside computer systems.

Privacy and Safety

- Don't go into chat rooms or send chain letters. If applicable, teachers can create discussion groups for communication among students for educational purposes.
- Users are not to open, use, or change files that don't belong to them.
- Students are not to reveal names, phone numbers, home addresses, social security numbers, credit card numbers, or passwords.
- Storage is never guaranteed to be private nor confidential since the device and the accounts themselves are the property of the Senatobia Municipal School District, and all documents are to be assumed non-confidential and subject to viewing by appropriate staff members if needed.

- If accessing a site and obscene, pornographic, or offensive material is seen, immediately exit the site and report the incident to the teacher.
- Staff is reminded that it's inappropriate to give out confidential information, and any other material that would be covered under the Family Educational Rights and Privacy Act (FERPA). Staff releasing confidential information, purposely or inadvertently, will be subject to penalties provided by existing SMSD policies and procedures.
- Users are monitored by the network filter with keywords flagged and appropriate staff notified.

Legal Property

- All trademark and copyright laws and license agreements are to be followed. Ignorance of the law is not immunity; when unsure, ask a teacher or parent.
- Plagiarism is a violation of board policy and includes graphics, movies, music, ideas, and text. Give credit to all sources used.
- Use of malicious software is prohibited and users who do so will be disciplined. Local, state, or federal laws that are violated will result in prosecution and/or disciplinary action by SMSD.
- SMSD retains the copyright to any material created and posted on the Internet or network by any employee or student while performing duties or coursework.
- Cyberbullying is not only a violation of district policy but also state law and will not be tolerated. Please report any cyberbullying to the school and/or district administration immediately.

Email and Electronic Communication

- Use appropriate language in communication.
- Do not transmit profane, obscene, or abusive material.
- Do not send chain letters, mass emails, or spam messages.
- All email and other communications sent and received should be related to educational needs and are subject to inspection by the district at any time.

Consequences

- Students will be responsible at all times for their account and device along with their appropriate use.
- Noncompliance with the policies of the district, including the ones in this handbook, will result in disciplinary action.
- Nothing done on a district device is considered confidential and can be monitored at any time by designated district staff to ensure proper use of resources.
- SMSD cooperates with local, state, and federal officials in any and all investigations concerning or related to violations of computer crime laws.

At Home Use

- Home usage of assigned student devices is encouraged.
- Users are to care for their device at home just like they do at school.
- Transport the device in the school-provided case. It must not be removed at any point.
- School district filtering will be provided for use with devices outside of school district buildings.
- All SMSD AUP policies are just as valid when students are at home while using an SMSD-owned device and login.

Protecting and Storing the Device

Device Identification

Student devices will be labeled by SMSD. They can be identified in three ways:

- District inventory sticker
- The student's user account
- The student's barcode identification sticker.

Account Security

- Students are required to use their school account with school devices and to protect the integrity of the account; do not give out the password to other students.

Storing the Device

- Students should take their assigned devices home every day after school, whether they're needed for homework or not.
- Do not store devices in vehicles; temperature and security issues may damage the device.

Devices Left in Unsupervised Areas

- Never leave a device in an unsupervised area.
- Unsupervised areas could be considered school grounds and campus, the cafeteria, computer labs, classrooms, hallways, and any other number of areas. Unsupervised areas are any public areas where the student is not.
- Contact a staff member immediately if an unsupervised device is found.
- Unsupervised equipment will be confiscated by staff and disciplinary action may result.

Repairing and Replacing Devices

Device Repair Costs and Insurance:

- First Intentional/Negligent Damage Occurrence: \$25
- Second Damage Occurrence: \$25 plus the cost to repair the device or fair market value and possible loss of take home privileges. Take home privileges may be removed at any time at the discretion of school administration.
- Third Damage Occurrence: \$25 plus the cost to repair the device or fair market value and loss of take home privileges. Take home privileges may be removed at any time at the discretion of school administration.
- Fourth Damage Occurrence: Fair market value to repair or replace the device.
- Lost or Stolen: Fair market value to replace the device. A police report should be filed if stolen.

Fair Market Value

Fair Market Value is determined by using the following formula: Device Cost - (Device age * \$25)

Broken Screen	Cost of Occurrence
Broken Keyboard	Cost of Occurrence
Power Adapter + Cord	Cost of Occurrence
Liquid damage to device	Cost of Occurrence
District Assigned Case	Cost of Occurrence

Prices can't be listed because the cost of replacement parts fluctuate depending on supply and demand. Senatobia Municipal School District reserves the right to charge for the entire replacement cost if negligence is determined.

Device Technical Support

The district employs technical support staff who can perform maintenance on damaged systems. Services provided include:

- Repairs
- Password resets
- User account support
- Warranty information and coordination

Do **NOT** take assigned student devices to any outside technician. They must be repaired by SMSD technicians.

Chromebook FAQs

What is a Chromebook?

Chromebooks are small, lightweight laptops that run a system called ChromeOS. The system looks like the Google Chrome browser and functions similar to it. They're fast, have a long battery life, connect to only WiFi, and are ideal for research and schoolwork. They're safer for minors because of a higher level of security built into the operating system coupled with regular ongoing updates to patch vulnerabilities. They're also easier to repair in the event of damage.

Can I install apps on my Chromebook?

Chromebooks don't actually run applications. Users can't install programs on them in the traditional sense. Things from the Chrome Web Store can be installed, but these are more like browser extensions or shortcuts.

Can I install things from the Chrome Web Store?

The district manages what can and can't be installed from the Chrome Web Store because of the possibility of misuse or cluttering. Even Chromebooks can be sluggish if too many apps are installed, so we try to protect our end users by pushing out the apps they need per their classroom teachers. If it's determined a student needs something special then it can be arranged, but the request has to come through the helpdesk system from staff.

What devices can I connect to a Chromebook?

- Mice
- Keyboards
- External monitors and projectors via HDMI or equivalent adapter
- Headsets/earbuds and microphones

Can the Chromebook be used anywhere?

As long as the user has an Internet connection, it can be used. If the user anticipates they won't have an Internet connection for some reason, they can mark the documents needed as 'available offline' while they have internet.

Can I use this like my cell phone?

The district Chromebooks don't have SIM cards built in, so they won't work when not used on WiFi.

Are we filtered on our Chromebooks?

Yes, they're filtered and can only be used with **senatobiaschools.com** accounts

What about the battery life?

Chromebooks have a longer battery life than Windows laptops because the OS has a small energy footprint. Users can expect at least 6.5 hours of use, but students are still expected to charge them every night to be ready for the next school day.

Technology Acceptable Use Policy (AUP)

Internet Use

Senatobia Municipal School District (SMSD) gives the privilege of Internet access to district staff, students, and guests. Each user, or in the case of a student, their parent or guardian, agrees to voluntarily release, hold harmless, defend, and indemnify (to compensate someone for harm or loss), SMSD and its officers, board members, employees, and agents for and against all claims, actions, charges, losses, and/or damages that come out of the use of the SMSD network, including but not limited to negligence, personal injury, wrongful death, property loss, or damage, delays, non-deliveries, misdeliveries of data, or service interruptions.

SMSD will cooperate with all local, state, and federal officials in any investigations related to illegal activities that were conducted on the SMSD Network, on any district device, and through any district user account.

Access on the SMSD network will be restricted to comply with the Children's Internet Protection Act (CIPA.) Web browsing will always be monitored and filtered, and records will be retained to ensure compliance.

Users are expected to respect the web filter and agree to not try to get around the web filter to access things which they're not allowed to access. Content and intended use of the material is the only determination of whether the material is appropriate or inappropriate, not on whether a website has been blocked or not. If a user thinks a site is unnecessarily blocked, the user can submit an unblock request through the filtering system or through the help desk system.

Each user is aware and understands that the information available from other websites may not be accurate. Use of any of the information from the Internet is at the user's own risk. SMSD makes no warranty of any kind, expressed or implied, in regard to the quality, accuracy, or validity of the data on the Internet.

SMSD Network Rules

- The person that an SMSD account is made for is responsible for that account at all times, including its proper use.
- Inappropriate use can possibly result in the cancellation of the privilege of use and/or disciplinary action.
- Consequences for any user who fails to comply with SMSD guidelines may include paying for damages, denial of access to the technology, detention, suspension, expulsion, or other remedies that fall under the school disciplinary policy and state or federal law.
- Any district employee who uses the SMSD network inappropriately is subject to disciplinary action, including dismissal.
- An SMSD network user should NEVER under any circumstance give their login information to another user nor allow another user to access their account unless communicating directly with a technology department employee who is assisting them.
- Schools can add any provisions to the SMSD AUP and can require additional parent releases and approvals, but in no case will any of those documents replace or take away from the SMSD AUP.
- Users must immediately report to SMSD authorities any attempt by another network user to engage in any inappropriate conversations or personal contact.
- Non-standard software needed to perform a specific job function MUST be brought to the attention of the Technology Department BEFORE it is purchased. If it's approved, those applications will be the sole responsibility of that office, and if the application is found to interfere with any required programs, applications, and/or utilities, the program will be disabled.

Acceptable Uses of Technology (though this isn't all inclusive)

A responsible user of district technology will:

- Follow the same rules of responsible and respectful behavior that they're expected to follow when they're offline.
- Treat school resources respectfully and tell staff if there's a problem with the resource's operation.
- Encourage positive and constructive discussion if allowed to use communicative and collaborative technology.
- Alert a teacher, administrator, or other staff member if they see threatening, inappropriate, or harmful content (including but not limited to images, messages, and posts) online.
- Use district technology at appropriate times, in approved places, and only for educational purposes.
- This isn't a complete list. That would be impossible. Users should utilize their own common sense and good judgment when using district technology.
- A good rule of thumb: if a user wouldn't want a staff member seeing it, it's likely not allowed on the network.

Unacceptable Uses of the Technology (though this isn't all inclusive)

A responsible user of district technology will NOT:

- Violate any kind of state or federal law (including copyright laws).
- Use profanity, obscenity, or language that would offend other people.
- Make personal attacks on other people, organizations, religions, or ethnicities.
- Create, access, download, store, or print files, images, or messages that are sexual in nature, obscene, or which offend or degrade others. SMSD administration invokes its rights to determine what is appropriate and inappropriate.
- Disrespect other peoples' privacy by posting personal contact information, such as work/home addresses, phone numbers, email, photographs, or names, online without obtaining that person's permission
- Transmit student information without the written permission of the parent/guardian of that student
- Use the SMSD Internet for commercial purposes, financial gain, personal business, to produce advertisement, for business service endorsement, or for religious or political lobbying
- Destroy or alter the files of another user
- View, take, or delete the files of another user
- This isn't a complete list. That would be impossible. Users should utilize their own common sense and good judgment when using district technology.
- A good rule of thumb: if a user wouldn't want a staff member seeing it, it's likely not allowed on the network.

Use of Outside Email Clients and Conditions for Using District Email Clients as a District Representative (Teachers, Administrators, etc)

Use of personal email by students and staff is not allowed.

Any official communication used for district business (for example, teacher to parent, teacher to student, staff to staff) **MUST** be via district email. This includes but isn't limited to teachers who guide extracurricular activities such as clubs, choirs, bands, and athletics.

Employees and students can only use the district email account for educational purposes or district business. Providing the district email address to anyone for any other purposes (such as using it as a return address for a non-business related website) is prohibited.

Filtering

An Internet filter is in place for on the SMSD network. The filter is a key component of the district network and aids the district's compliance with CIPA, allowing Internet access while restricting access to unwanted material in the following categories (though these aren't the only things:)

- Pornography
- Gambling
- Illegal drugs
- Online merchandise
- Hate speech
- Criminal Skills
- Alternative Journals
- Other undesirable content that violates the AUP

The filter is managed with the help of a 3rd party company specializing in K12 education to ensure it's always as accurate and protective as possible; however, filtering is never 100% accurate in preventing access to inappropriate sites. Inappropriate sites are added to the Internet daily, and it's impossible to catch them all. Every effort is made by the district to ensure students can't access inappropriate material.

Any attempt to bypass the Internet filters is a violation of this Acceptable Use Policy and will be subject to disciplinary action, including denial of access to technology, detention, suspension, expulsion, termination of employment, or other remedies that would apply under the school's disciplinary policy and state or federal law.

Workstation Monitoring

Data transferred over the SMSD network can be monitored at any time. The person sending any data or receiving requested data, in violation of any established policy, may be held liable for said data. The appropriate authorities will be notified if the activity is in violation of any law, state or federal.

Data stored on district-owned equipment, on a district account, or any other district file storage apparatus, whether that apparatus is physical or digital, is the property of SMSD and may be archived and preserved by the district for however long the district chooses. The data includes but isn't limited to email, text documents, digital photographs, music, and other digital or electronic files. If a workstation continues to try to access inappropriate sites, that workstation will be remotely monitored and the person using that workstation will be reported to the administration of the school.

Technologies Covered

SMSD may provide access to the Internet, computing devices, video conferencing devices, email, and a plethora of other technology equipment and opportunities.

This AUP applies to all district-owned technology utilizing the SMSD network, the SMSD Internet connection, and/or private networks, or Internet connections accessed from district-owned devices or logins at any time.

This AUP also applies to privately-owned devices while they access the SMSD network, the SMSD Internet connection, and/or private networks, or Internet connections while on school property or while participating in school functions or events off campus.

This document covers all technologies currently available and those that will be implemented in the future.

Email

Employee and student SMSD email is the property of the district, but it is the responsibility of the employee and student to maintain and secure the account.

Employees and students are not to use their district email account for personal communications.

Security

Users are expected to take reasonable security safeguards from online threats while on the SMSD network. This means a user is not to open or distribute infected files or programs, and they're not to open files or programs that aren't verified to be virus-free, that they weren't expecting, or from an unknown origin. Users should never share personal information.

If a user believes a device they are using might be infected with some type of malicious software, they should immediately alert the technology department via helpdesk ticket or, in the case of a student, have a staff member submit a helpdesk ticket for them. Users must not attempt to remove the threat themselves.

Online Etiquette

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

They should recognize that along with valuable educational content is also unverified, incorrect, or inappropriate content, and those users should only use known and trusted sources when conducting research via the Internet.

Users should not post anything they wouldn't want students, parents, teachers, colleges, colleagues, or employers to see because once something is online, it cannot be retracted and can be shared in ways and places that were never intended and that can never be erased.

Plagiarism

Users should never plagiarize (use something as their own without citing the original creator) content. Items that can be plagiarized include words, images, videos, and many other forms of media from the Internet or

other published or unpublished sources. Users should never take credit for work that is not theirs or pretend they're the author of something they did not create.

Information from the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including but not limited to phone numbers, addresses, social security numbers, birthdates, or financial information without adult permission. Users must recognize that communicating over the Internet brings both anonymity and the associated risks and should carefully guard their personal information along with that of others. Users should never meet anyone in person they've met online without parental permission and presence.

If users see something that makes them concerned for their own safety or the safety of someone else, they should bring it to the attention of an adult.

Cyberbullying

Cyberbullying including, but not limited to, harassment, flaming, unfair criticism, impersonation, outing, tricking, excluding, and cyber stalking are unacceptable and will not be tolerated. Users shall not send emails or post comments with the intent to do any type of harm, be it physical, mental, or emotional, and shall not create a hostile school environment for any individual.

Engagement in cyberbullying of any kind will result in disciplinary action, and in some cases, will be considered a crime. Users must always remember that online activities will be monitored.

All students must be educated about appropriate online behavior, including interacting with other people on social networking sites and in chat rooms, along with cyberbullying awareness and response.

Social Media

The Senatobia Municipal School District has a policy that addresses social media, which applies to all employees and students. By signing this AUP, users are acknowledging they have read and agree to abide by the social media guidelines. See SMSD policy GABBA social media. <https://senatobia.msbapolicy.org/>

Limitation of Liability

SMSD will not be responsible for damage or harm to persons, files, data, or hardware because while the district employs filtering and other safety and security mechanisms and attempts to ensure they're used properly, it cannot and will not guarantee their effectiveness.

The district will not be responsible or liable in any way for unauthorized transactions conducted over the SMSD network.

The web traffic viewed over the district network may be viewable by the filtering company. The district whitelists local and national banks but can make no guarantee the bank being used is whitelisted.

Violations of the AUP may have disciplinary consequences such as:

- Suspension of technology privileges
- Notification of parents
- Detention or suspension from school or school-related activities
- Employment disciplinary action up to and including termination of employment
- Legal action and/or prosecution

Employees, students, and parents/guardians shall be required to sign the Senatobia Municipal School District's Acceptable Use Policy before Internet or network access will be allowed.

Internet Safety and Cyberbullying Policy

The policy of Senatobia Municipal School District is as follows:

- Prevent user access and/or transmission of inappropriate material via SMSD Internet, email, and/or other forms of direct electronic communications over its network
- Prevent unauthorized access or other unlawful online activity
- Prevent unauthorized online disclosure, use, or spread of personal identification information (PII) of minors
- Comply with the Children's Internet Protection Act (CIPA) [Pub. L. No. 106-554 and 47 USC 254(h)]

Definitions

Key terms are as defined in CIPA

Access to Inappropriate Material

To the extent practical, technology protection measures, otherwise known as 'Internet filters', shall be used to block or filter Internet or other forms of electronic communications and access to inappropriate information.

As required by CIPA, blocking shall be applied to any material deemed harmful to minors, such as visual depictions of material deemed obscene or child pornography. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

As much as practical, steps shall be taken to promote the safety and security of all users of the SMSD network when using email, chat rooms, instant messaging, and any other forms of direct electronic communication.

Prevention of inappropriate network usage includes:

- Unauthorized access such as 'hacking' and other unlawful activities
- Unauthorized disclosure, use, and spreading of PII regarding minors

Education, Supervision, and Monitoring

It is the responsibility of all members of SMSD's staff to educate, supervise, and monitor the correct usage of the network and access to the Internet in accordance with the AUP, CIPA, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or modifying of any protection measures shall be the responsibility of the Technology Coordinator or designated representatives. SMSD or designated representatives will provide age-appropriate training for students who use SMSD's Internet facilities. The training will be designed to promote the district's commitment to:

- The standards and acceptable use of Internet services as set forth in the district's AUP.
- Student safety with regard to:
 - Safety online
 - Appropriate behavior online, on social media, and in other communicative software
 - Cyberbullying awareness and response
- Compliance with E-Rate requirements of CIPA

Following receipt of the training, the appropriate personnel will document that the student has received the training.

LEGAL REFERENCE: USAC; CHILDREN'S INTERNET PROTECTION ACT

Student/Parent/Guardian Technology Agreement 2023/2024

I, _____ (name, printed) as a borrower of an SMSD device:

- Have signed the SMSD Technology Agreement and agree to follow the policies established in the Student Technology Handbook.
- Will follow rules and guidelines listed in the handbook for the proper care of all my devices.
- Agree to pay a fee should I damage my device.
- Understand and agree that if the device is lost or damaged, I will be responsible to pay for repair or replacement of the device.
- Understand that if I'm not responsible and fail to follow the policies, SMSD may remove the device from my possession.
- Will report any problems or issues I discover while using the device.
- Understand that an SMSD device is an instructional tool, and I'm to use it for nothing BUT schoolwork.

Guidelines for Proper Care of the Device

1. I won't loan my device to anyone.
2. I won't remove any labels, stickers, cases, or screen protectors that were placed on the device without school permission.
3. I won't write on or deface in any way, including by applying stickers, to my device. I can place stickers on the case.
4. I will care for the device at all times, including but not limited to:
 - a. Not eating or drinking around the device
 - b. Not exposing the device to temperature extremes
 - c. Not attempting home repair or taking the device to non-SMSD technicians
 - d. Using the correct charger to charge the device
5. I will properly secure the device at all times and never leave it unsupervised in public, including these situations though not limited to them:
 - a. Unattended in an unlocked classroom, locker, or during sports practice
 - b. In a vehicle

Internet Access Agreement

In order for a student to gain access to the Internet, the student and student's parent(s) / guardian(s) must sign an Internet Access Agreement.

The superintendent is authorized to amend or revise the following board-approved initial administrative procedure as he/she deems necessary and appropriate consistent with this policy. The superintendent is further authorized to amend or revise the Internet Network Access Agreement with the advice of board counsel.

It must be understood by all concerned that the global and fluid nature of the Internet network's contents make it extremely difficult for the board to completely regulate and monitor the information received or sent by students. As such, the board cannot assure parents that students will be prevented from accessing undesirable materials or sending or receiving objectionable communications.

Student Name: Last_____ First_____

Parent Name: Last_____ First_____

Address: _____

Parent Email: _____

Parent Phone: _____

The Senatobia Municipal School District (SMSD) Acceptable Use Policy (AUP) allows student use of technology inside and/or outside of the classroom. SMSD may provide Internet access, computing devices, video conferencing software, digital learning capabilities, and much more.

I have reviewed the SMSD Technology Handbook and understand the rules and guidelines for the following:

1. District Technology Goals
2. Acceptable Use Policy
3. Use of District Technology / Internet Use Agreement
4. Financial Terms of Device Agreement

The student is always responsible for the care of their assigned device. If my student violates the policies, guidelines, and rules agreed to in the SMSD Student Technology Handbook, I understand their privilege to use technology may be restricted or removed, and they may face disciplinary action.

I understand I will also be held responsible for paying for the loss, damage, or repair of my student's device, no matter where the damage occurred, whether at school, at home, in public or private, or when the device was being transported.

The device remains the property of SMSD, and students are borrowing them for educational use. In case the assigned device listed below can't be repaired, SMSD has the right to assign a replacement device. A message about this will be sent through SchoolStatus so the parent will be aware.

At the end of the school year or upon transfer of the student out of the district, parents and students agree the device should be returned in the same condition it was issued outside of reasonable wear and tear or the parent will pay the repair or replacement cost.

Signatures

Parent/Guardian Signature

Student Signature

Date

School

Grade Level

Asset Number

Senatobia Municipal School District

Student Device Acceptance Form

I understand and agree that the device or any other equipment that the district provides to me are the property of SMSD. I agree to this and the terms and conditions of the SMSD Device User Agreement and also those of the SMSD Student Technology Handbook.

I understand and agree that I must immediately report any damage, loss, or theft of my device to teachers, staff, or administrators. I also understand that if my assigned device is damaged, stolen, or lost, my parents or guardians will pay for the repair or replacement of the device, no matter where the damage, theft, or loss took place, whether at home, at school, in public or private, or while transporting the device.

I understand the district may issue me a replacement device if my device can't be repaired and my parents or guardians will be notified through SchoolStatus.

I will participate in a training session/class about appropriate online behavior, including interacting with other people on social media and in chat rooms, and I will also be trained how to deal with cyberbullying, both how to be aware of it and how to responsibly respond.

I understand that if I violate the terms and conditions set out in the Student Technology Agreement and SMSD Student Technology Handbook, I may have my privileges restricted or revoked, and the district may take my issued device or any other district devices back.

Items Received:

Device _____ (asset number)
Power Supply
Device Case

New
New
New

Condition

Used
Used
Used

Student Signature:

Date:

Parent/Guardian Signature:

Date:
