

STUDENT TECHNOLOGY ACCEPTABLE USE AND INTERNET SAFETY

The St. Martin Parish School Board offers Internet access for students' use. This document is the *Acceptable Use* policy for student use of technology, Internet, and technological resources. This Internet system has been established for a limited educational purpose to include classroom activities, career development, and limited high-quality, self-discovery activities, which enhance learning and teaching. It has not been established as a public access or public forum. The St. Martin Parish School Board has the right to place reasonable restrictions on the material accessed or posted, require the training needed before a student is allowed to use the system, and enforce all rules set forth in the school code and the laws of the state. Further, students may not use this system for commercial purposes to offer, provide, or purchase products or services through the system or use the system for political lobbying. Access to the Internet, technology systems, and resources is available to all St. Martin Parish students. It is a privilege afforded to students who agree, along with their parents/guardian, to abide by the *Student Technology and Internet Acceptable Use* policy. Should a parent/guardian desire to prohibit their child's access to the internet, the responsibility rests on the parent/guardian to properly execute the Denial of Permission form located in the Student Discipline Handbook. If the school does not receive the Denial of Permission form, parental permission to use the technology systems of the School Board will be assumed, and this permission shall include access to the internet and email systems, permission to publish student work to classroom websites, and permission to have unidentified photos of the student published to classroom websites.

It is the policy of the St. Martin Parish School Board to:

1. Prevent user access over its technology network to, or transmission of, inappropriate material via any forms of communications;
2. Prevent unauthorized access and other unlawful online activity, network activity and/or use of technology resources and systems;
3. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
4. Comply with the *Children's Internet Protection Act* [Pub. L. No. 106-554 and 47 USC 254(h)], Federal and state laws, including, but not limited to, Louisiana's cyberbullying laws.

Students found in violation of this policy may have these privileges revoked along with other suitable penalties in accordance with the St. Martin Parish School Board's Discipline policies.

KEY TERMS AS DEFINED IN THE CHILDREN'S INTERNET PROTECTION ACT (CIPA)

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the *Children's Internet Protection Act* (CIPA), blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the St. Martin Parish Public Schools online computer network when using electronic mail, forums, and other forms of direct electronic communications. Specifically, as required by the *Children's Internet Protection Act* (CIPA), prevention of inappropriate network usage includes:

1. Unauthorized access, including "hacking," and other unlawful activities; and
2. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Supervision and Monitoring

It shall be the responsibility of all St. Martin Parish School Board personnel to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the *Children's Internet Protection Act* (CIPA).

Harmful to Minors

The term *harmful to minors* means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Sexual Act; Sexual Contact

The terms *sexual act* and *sexual contact* have the meanings given such terms in section 2246 of Title 18, United States Code

Technology Protection Measure

The term *technology protection measure* means a specific technology that blocks or filters Internet access to visual depictions that are:

1. *Obscene*, as that term is defined in section 1460 of title 18, United States Code;
2. *Child pornography*, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

PERMISSIBLE USES

Access to the Internet shall enable students to explore thousands of libraries, databases, museums, and other repositories of information. Families should be aware that the school and District websites may contain links that are maintained and controlled by third parties. Because some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive, School Board personnel shall make every effort to filter, screen, and research links for appropriateness. St. Martin Parish School Board is not responsible for the content in the linked site, any link contained within the linked site, or any changes or updates to the linked site that changes its appropriateness.

The St. Martin Parish School Board believes that the benefits to students from access to the Internet in the form of information resources and opportunities for collaboration exceed the disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. Therefore, we support and respect each family's right to decide whether or not to allow access.

This policy also grants the following:

- Permission for students to access the Internet at school
- Permission to access and use a safe, District-approved, monitored electronic communication and learning resource account (if permitted by teacher and school administrator) [grades 3-12 only]
- Permission for student's name, schoolwork, pictures/videos of child to be published to the classroom, school, or district website [Personal information (i.e.

address, phone number, social security number) about the student shall not be included in a webpage]

- Permission for student to participate in e-Learning activities in the classroom (i.e. Google Meet/Classroom) with the understanding that the child's image may be visible to teacher and students in partnering classroom
- Permission for student to receive electronic communication from club sponsors, coaches, etc. (i.e. email, text messages, phone call)

Any parent wishing to revoke/suspend/or deny student permission(s) must opt out in writing.

EXPECTATIONS

- Students shall comply with District standards and the specific rules set forth below.
- Students shall display appropriate behavior on the school's computers and network.
- Each student shall be personally responsible for his/her actions in accessing and utilizing the school's computer resources.
- Students shall be advised never to access, keep, or send anything that they would not want their parents/guardian or teachers to see.
- The use of the network is a privilege, not a right, and may be revoked if abused.
- Students shall be provided training, annually, on St. Martin Parish District CIPA policies. Training shall address key issues such as cyberbullying, social networking dangers, Internet/digital safety, and emerging technologies which may endanger children while using the Internet.
- In addition, the School Board, in conjunction with local law enforcement agencies, shall develop and distribute age and grade appropriate information to each student regarding Internet and cell phone safety and online content that is a threat to school safety. The information shall include the following:
 - Instruction on how to detect potential threats to school safety exhibited online, including posting on any social media platform
 - Visual examples of possible threats
 - The process for reporting potential threats, which shall be in accordance with the procedures referenced in policy *EBBB, School and Student Safety*.

Such information shall be either distributed to or explained to students and school personnel at the beginning of each school year and shall be posted on an easily accessible page of the School Board's website and the website of each school.

If information reported to a school is deemed a potential threat to school safety, the school shall present the written form and any further evidence to local law enforcement.

RULES

Privacy

Network and/or computer storage areas are like school lockers. The computer equipment is School Board property. Network administrators may access and review communications to maintain system integrity and ensure that students are using the system responsibly.

- The student shall not post personal or private contact information about self or others. Personal contact information may include, but not limited to, social security number, home address, home phone number, personal email address, etc. This also includes photographs of oneself and others, as well as student work.
- While accessing the St. Martin Parish School Board's technology system, the student shall not agree to meet with someone they have met online.
- The student shall promptly disclose to the teacher or other school employee any message received that is inappropriate or makes the student feel uncomfortable.

Inappropriate Network Usage

- The student shall not use the School Board's technology network and equipment to download, send, receive, view, or create obscene or pornographic or harmful to minors images or files.
- The student shall never download or install any commercial software, shareware, or freeware onto network drives or disks, unless given written permission from the Network Administrator.
- The student shall adhere to all copyright laws. Violations include, but shall not be limited to, copying or reproducing work that is protected by a copyright, files/documents created by others, and copyrighted multimedia content such as music and video clips accessed through file sharing software).
- The student shall not attempt to gain unauthorized access to the St. Martin Parish School Board's technology system (i.e. Forum, JCampus, OnCourse, etc.) or to any other computer system via the School Board's computer system or go beyond the authorized access. This includes attempting to log in through another person's

account or access another person's files. These actions are illegal, even if only for the purposes of *browsing*.

- The student shall not make deliberate attempts to disrupt the computer system's performance, destroy data by spreading computer viruses or by any other means. This includes the destruction and vandalism of computer equipment and its components.
- The student shall not use the system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, participating in virtual games that mimic illegal activities, or threatening the safety of others, etc.
- The student shall not pursue or otherwise access information on weapons and the manufacture or purchase of weapons for purposes other than assigned class research.
- The student shall not use the School Board's technology system or network for personal acquisitions such as shopping, trading stocks, any form of financial gain unrelated to the mission of the school district, personal entertainment, and on-line gambling.
- The student shall not use the School Board's technology system or network to play non-educational, student-initiated games.
- The student shall not use the School Board's technology system or network to conduct plagiarism. *Plagiarism* is using another person's ideas or writings and presenting them as one's own.
- The student shall not use the School Board's technology system to commit the act of cyberbullying. *Cyberbullying*, for the purposes of this policy is the harassment, intimidation, or bullying of a student on school property by another student using a computer, mobile phone, or other interactive or digital technology or harassment, intimidation, or bullying of a student while off school property when the action or actions are intended to have an effect on the student when the student is on school property.

Inappropriate materials or language

- The student shall not use bullying, intimidating, obscene, profane, lewd, vulgar, rude, inflammatory, threatening, abusive, impolite, disrespectful, or sexually explicit language to communicate. Materials which are not in line with the rules of school behavior should not be accessed. Should students encounter such material by accident, they should report it to their teacher immediately and turn off the monitor.
- The School Board's computer system is considered a limited forum, similar to the

school newspaper, therefore the School Board may restrict speech for valid educational reasons.

- Restrictions against inappropriate language apply to public messages, private messages, and material posted on web pages, social networking sites, and teaming management sites (i.e. Google Classroom, Class Flow, Schoology, etc.)
- The student shall not access, post, distribute, forward, print, or store materials using language that is inappropriate to the educational setting or disruptive to the educational process.
- The student shall not use the Internet and/or any other electronic device or system, on or off campus, that subsequently causes substantial disruption to the educational environment, interferes with the rights of others, or can be considered a threat.
- The student shall not engage in personal attacks, including prejudicial or discriminatory attacks, even if made in a joking manner.
- The student shall not harass another person. *Harassment* is persistently acting in a manner that distresses or annoys another person. When requested by another to stop communication in the form of messages, e-mail, or other means of electronic contact, the student shall do so immediately.
- The student shall not knowingly or recklessly post false or defamatory information about a person or organization.
- The student shall not use his/her access to review, upload, download, store, print, post, or distribute materials that:
 - Are pornographic, obscene or sexually explicit.
 - Use language or images to advocate violence or discrimination towards other people (hate literature); a special exception may be made for hate literature if the purpose of access is to conduct educational research and both the teacher and parent have approved.
 - Contain images of individuals engaged in any illegal act or violate any local, state, or federal statute/law.

Electronic Communication and Learning Resource Accounts

- Students shall not use or access unapproved personal email or electronic communication accounts at school. (i.e. Yahoo, Hotmail)
- Students shall only be allowed to access and use a District-approved school

electronic communication and learning resource account which is managed, monitored, and filtered.

- Students shall not be allowed to correspond with others beyond restrictions set by the teacher.
- Student electronic communication and learning resource accounts shall be restricted by district and/or teacher limits.
- Unsolicited communication (i.e. spam) shall be filtered and restricted.

Mobile Devices and Expectations

The term *mobile device*, for the purpose of this policy, refers to, but is not limited to, handheld devices provided by the St. Martin Parish School Board and allowed in the school system and on the St. Martin Parish School Board's network for educational purposes. Some examples are: iPads, iPods, Tablets, Chromebooks, Laptops, etc. Said mobile devices are the property of St. Martin Parish School Board and must be used in accordance with St. Martin Parish School Board's *Acceptable Use* policy, procedures, and all applicable laws. Only District-issued mobile devices shall be allowed in the schools and on SMPSPB's network. All others shall be prohibited. Students are allowed to use the assigned St. Martin Parish School Board issued mobile device off campus for remote and/or educational purposes.

- The mobile device is School Board property and all users shall follow the *Technology Acceptable Use and Internet Safety* policy.
- The mobile device shall be used in a responsible and ethical manner.
- Passwords shall not be changed or altered on the device.
- The mobile device(s) should be checked in/and out yearly to the student through the district's inventory platform.
- The mobile device is expected to be in possession of the assigned student while working in person on-site
- Devices shall be housed in a secure designated area at all times.
- All software/applications shall be District approved.
- All downloading/syncing shall be done in accordance with District procedures.
- Mobile devices shall always be within the protective case provided, if applicable.
- The St. Martin Parish School Board shall have the right to review items for appropriateness and to limit or revoke access to mobile devices at any time for any reason.

MISUSE

- The student shall use the St. Martin Parish School Board's technology system only for educational and career development activities and limited, high-quality, self-discovery activities.
- The student shall not download files and/or stream music.
- The student shall not engage in spamming. *Spamming* is sending an annoying or unnecessary message to a large number of people.

DUE PROCESS AND CONSEQUENCES

Users of the School Board's computers, network, and Internet are held personally responsible for actions in accessing and utilizing available resources. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the School Board's computer system or the Internet may result in one or more of the following consequences:

1. Suspension or cancellation of use and access privileges;
2. Payment for damages and repairs;
3. Disciplinary actions in accordance with other appropriate School Board policies as stated in the St. Martin Parish *Student Handbook* including:
 - A. Detention, suspension, and or expulsion from school;
 - B. Civil or criminal liability under other applicable laws;
 - C. Restitution for restoration costs.

LIMITATION OF LIABILITY

Although the St. Martin Parish School Board enforces a policy of technology and Internet safety and employs technology protection measures to block and or filter inappropriate material from student and employee access, the School Board shall not be responsible for damages suffered, including but not limited to, loss of data or interruptions of service. The School Board shall not be responsible for the accuracy or quality of the information obtained through its services or stored on its system. The School Board shall not be responsible for any costs or liabilities arising from the unauthorized use of the system.