

ST. MARTIN PARISH SCHOOL DISTRICT
TECHNOLOGY and INTERNET ACCEPTABLE USE POLICY
For Employees

A. PURPOSES

The purpose of this policy is to set forth the procedures, rules, guidelines and code of conduct for the use and monitoring of the St. Martin Parish School District's computer equipment, network, and Internet access via the district network.

The St. Martin Parish School District offers employees access to the school district's technology network, which includes computer and technology equipment, the district's network, the Internet, email, access to software systems and other forms of electronic communication. This access is provided to assist employees in carrying out the educational business of St. Martin Parish Schools, conducting research, taking advantage of other repositories of information and communicating, as well as, exchanging ideas with other Internet users around the world. We believe the benefits of access to the Internet in the form of information resources and opportunities for collaboration exceed the disadvantages. However, employees are expected to observe the rules, guidelines, and responsibilities outlined below:

- Use of such technology is a necessary element of St. Martin Parish School District's Mission, but is furnished to employees as a privilege, not a right.
- Information posted on the Internet is public and permanent. Email and other communications transmitted via the district's network and/or stored on district resources are not private and may be reviewed by district technology personnel to ensure that all guidelines are being followed.
- Users should refrain from activities that annoy others or disrupt the educational experiences of their peers.
- Teachers shall ensure students are provided age and grade appropriate instruction regarding St. Martin Parish District CIPA policies and Internet/digital safety. Such instruction shall include appropriate online behavior, including interacting with other individuals on social networking websites and chat areas, and cyberbullying awareness and response, emerging technologies which may endanger children, as well as areas of concern as authorized in state and federal law. Instruction will be incorporated within lesson plans. Students are to be informed by staff of their rights and responsibilities as users of the district network prior to gaining access to that network, either as an individual or as a member of a class or group.
- As per the FCC revisions of section 54.20(c)(1)(i) of CIPA, teacher/employee and/or staff shall monitor, not rely solely on the district's filtering and monitoring system, all student technology and Internet use to ensure student compliance with the district's Student Acceptable Use Policy, student's access to age appropriate, educational material and assure inappropriate material is not being accessed by minors both on and offline.
- Teacher/employee and/or staff shall report any inappropriate access or harmful material by minors and additional access restrictions as appropriate when observed during monitoring to school administration and district technology department.
- School administration, teacher, employee and staff are to ensure the presence of teacher and/or other appropriate district personnel when students are accessing the Internet and/or technology including, but not limited to, the supervision of minors when using any form of electronic communication. The use of electronic communication venues is determined by appropriate building administrator and district procedure/policy. Some forms of direct electronic communications may be filtered and/or blocked as deemed necessary to ensure the safety of such students.
- All electronic communication to a student must be related to educational services. Such communication shall be reported by the employee on the Employee/Student Communications

Form.

- All passwords, system logins and accounts are to be used **only** by the authorized user of the account, for authorized district purposes and in accordance with the job duties outlined by the district.
- Employees are responsible for “backing up” files and reasonable care of equipment assigned to them.
- Failure to comply with this policy could result in loss of access privileges and/or appropriate disciplinary action.
- Teachers and staff will participate in annual training on Internet/digital safety, St. Martin Parish School District standards, student data privacy and policies, and acceptable use of Internet services and technology usage. Safety on the Internet training will include, but not limited to, appropriate behavior while online, on social networking websites and in chat areas, cyberbullying awareness and response and compliance with the E-Rate requirements of the Children’s Internet Protection Act (CIPA).
- Employees are responsible for complying with all student and employee data privacy, confidentiality and sharing laws and district policies.
- No personal or student information which is protected by the Family Educational Rights and Privacy Act shall be disseminated on or through St. Martin Parish School Board’s technology systems and networks, including but not limited to the Internet.
- No personal or confidential employee information which is protected by law shall be disseminated on or through St. Martin Parish School Board’s technology systems and networks, including but not limited to the Internet

B. 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 those allowed in the school system and on SMPSB’s network for educational purposes. Mobile devices are provided by SMPSB for the purpose of carrying out the educational business remotely and/or in a mobile fashion. Some examples are: iPads, Laptops, Tablets, Chromebooks, etc. Said mobile devices must be used in accordance with SMPSB’s Acceptable Use Policy, Procedures, and all applicable laws. Use of these mobile devices, as well as access to the network, the Internet, and email are a privilege, not a right. These devices are allowed and intended to support learning and increased access to technology.

EXPECTATIONS

- The mobile device users will follow the St. Martin Parish School Board Technology and Internet Acceptable Use Policy.
- As per district procedures, all SMPSB mobile devices are to be set up through district management systems and logged/tagged.
- The mobile device(s) should be checked in/and out yearly to the staff through the district’s inventory platform.
- The mobile device is expected to be in possession of the assigned staff while working in person on-site
- The mobile device should be used in a responsible and ethical manner.
- Passwords should not be changed or altered on the device.
- Devices should be housed in a secure designated area at all times.

- All software/Apps must be district approved.
- All downloading/syncing should be done in accordance with district procedures.
- Mobile devices should always be within the protective case provided, if applicable.
- All mobile devices are managed and monitored by the St. Martin Parish School District.
- SMPSB has the right to review items for appropriateness and to limit or revoke access to mobile devices at any time for any reason.

C. LIMITED EDUCATIONAL PURPOSE

- The St. Martin Parish computer system has been established for limited “educational purposes”. The term “educational purposes” includes classroom activities, career development, and limited high quality, self-discovery activities.
- It has not been established as a public access or public forum. Uses which might be acceptable on a private, personal account on other computer systems may not be acceptable on this limited purpose network.
- The St. Martin Parish School Board has the right to place reasonable restrictions on the material you access or post and the training required before you are allowed to use the system. St. Martin Parish School Board also reserves the right to enforce all rules set forth in the parish’s Employee/Teacher Handbook and the laws of the state.
- The communications and computer storage of users of the school district’s computer system may be routinely monitored and reviewed by network administrators to maintain system integrity and ensure responsible use.
- This system may not be used for commercial purposes to offer, provide, or purchase products or services, or for political lobbying.
- Student access to the Internet is granted only to those students who have signed a Student Technology Acceptable Use and Internet Safety Policy and have been informed by staff of their rights and responsibilities as users of the district network. Each time a student enters a new school, updated signatures must be obtained. Signatures remain valid and, in the student’s, cumulative folder until and unless the parent revokes the child’s privileges in writing or through disciplinary action taken by the school. Access level/permissions will also be recorded in the district Student Information System on the student’s demographic record.

D. ACCEPTABLE USES

The St. Martin Parish School District network may be used for the following:

- Creation of files, projects, web pages and other forms of educational technology material using network resources in support of educational research;
- Participation in district-approved blogs, other electronic communication venues, discussion boards, groups, e-Learning and email that support educational research;
- The online publication of original educational material, curriculum-related materials and student work;
- Should an employee see any unacceptable materials or inappropriate use, he/she shall notify the site administrator or supervisor immediately. Report any instances where the Acceptable Use Policy or security may be violated. Report inappropriate Internet Web sites to Administration so the district technology department can block access to the site.
- If there is any doubt as to the appropriate use of a District-provided electronic system, review the

use in advance with a supervisor.

E. UNACCEPTABLE USES

The following uses of the St. Martin Parish School District's computer system are considered unacceptable:

1. Personal Safety

- Employees should not post personal or private contact information including, but not limited to, social security numbers, home addresses and telephone numbers, school and work addresses, personal email addresses, etc. on websites, blogs, podcasts, videos, wikis, email or as content on any other electronic medium.
- Employees should not use with or refer students to social networking sites and other sites not approved/recommended by the St. Martin Parish School Board
- Employees should not post videos of school activities to YouTube or other non-approved websites, without permission from the St. Martin Parish School Board
- Employees should not use non-approved third-party sites for student email, blogging, discussion boards, etc.
- Employees should not post pictures or names of students on any class, school or district website unless the appropriate permission has been verified according to district policy
- Employees should not share passwords, log-ins, access to school board accounts, or use another person's password, log-in, or access
- Employees should not use the "remember password" feature of Internet browsers
- Employees should log off, if leaving the room (i.e. SIS, lesson plans, testing platforms, e-mail, etc.)
- Employees should not leave electronic gradebook open and unattended while students are in the classroom

2. Illegal Activities

- Employees should not attempt to gain unauthorized access to the St. Martin Parish School District's computer system or to any other computer system via the district's computer system or attempt to defeat or bypass the district's filter or conceal Internet activity. 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".
- Employees should 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/network equipment and its components.
- Employees should 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, threatening the safety of others, etc.
- Employees should not use the system to engage in non-school-related communications with students.
- Employees should use the platforms provided/approved by the St. Martin Parish School District for communicating with students (refer to District's approved resource list)
- All other electronic communications should be documented on the Employee/Student Electronic Communications Form. [Electronic Communication includes, but not limited

to voice, text-based devices and computers, and those that facilitate indirect communications using an intermediate method, including but not limited to Internet-based-social networks.]

- Employees will 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 use of on or off campus resources, including websites or social networking sites, etc. that subsequently cause “material disruption” at school is prohibited
- Employees should not pursue or otherwise access information on weapons and the manufacture or purchase of weapons.
- Employees should not use the network or school board equipment for commercial, political, personal or private gain
- Employees should not use the school district’s computer system 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.
- Employees should not attach **unauthorized equipment** to the district network, including, but not limited to laptops, wireless routers, access points, etc. [If found, prohibited items will be confiscated by district personnel]
- Employees should not download, install, add as an extension or use games, audio files, software, apps or other applications without consent from the Technology Supervisor or Network Manager or that has not been district approved
- Employees should not use the district’s internal network that incurs expenses to the school and/or district without prior approval of expenditure.

3. Inappropriate Access to Material

Employees should **not use 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).
- contain harassment of any kind, discriminatory jokes and remarks, defamation, cyber bullying, etc.
- engage in any illegal act or violate any local, state, or federal statute or law
- facilitate hacking, cracking, vandalizing, introducing viruses, worms, Trojan horses, time bombs, ransomware, etc. that inhibit operation of a computer or network
- overwhelm the network, including but not limited to chain letters, network games, mass copying of files for no specific reason, etc.

4. Inappropriate Language

- The school district’s computer system is considered a limited forum, similar to the school newspaper; therefore the district may restrict your speech for valid educational reasons
- .Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.
- Employees should not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language.
- Employees should not access, post, distribute, or store materials using language that is

- inappropriate to the educational setting or disruptive to the educational process.
- Employees should not engage in personal attacks, including prejudicial or discriminatory attacks.
 - Employees should 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, you will do so immediately.
 - Employees should not knowingly or recklessly post false or defamatory information about a person or organization.

5. Plagiarism and Copyright Infringement

- Employees should not use the school district's computer system to conduct plagiarism. Plagiarism is using another person's ideas or writings and presenting them as your own.
- Employees should not violate copyright laws by reproducing work that is protected by a copyright. This includes copyrighted multimedia content such as music and video clips accessed through unapproved sites.
- Employees should not copy, transfer or duplicate software owned by or registered by St. Martin Parish School District.
- Employees should not transmit or download any material in violation of any national, state or district regulation.

6. Respecting Resource Limits

- Employees should use the St. Martin Parish computer system only for educational and career development activities and limited, high-quality, self-discovery activities.
- Employees should not download large files unless absolutely necessary. If necessary, you will download these files at a time when the system is not being heavily used and remove these files when no longer needed.
- Employees should not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
- Employees should subscribe only to high quality discussion group mail lists that are relevant to your education or career development.

7. E-Mail and Electronic Communication and Learning Resource Accounts

- Employees should check e-mail frequently and delete unwanted messages promptly.
- Employees of St. Martin Parish are responsible for the content of their e-mail messages and attachments
- Employees should not allow students access to the employee's email account
- Students are only allowed to access and use a district-approved, school electronic communication and learning resource account which is managed, monitored, and filtered (i.e. Google Workspace accounts set up by SMPSB, Google Classroom, Remind, LMS)

F. DUE PROCESS AND CONSEQUENCES

Users of the school district's computers, network, and Internet are held personally responsible for their own 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 district'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 district policies as stated in the St. Martin Parish Policy Handbook (IFBGA)

G. LIMITATION OF LIABILITY

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

EMPLOYEE/STUDENT ELECTRONIC COMMUNICATIONS FORM

| | | | |
|---------------------------------------|------------------|---|--|
| Date | | Name of School | |
| First Name | | Last Name | |
| Position | | Email Address | |
| Name(s) of Student(s) Or Group | | | |
| | | | |
| | | | |
| | | | |
| Contact Initiated by: | Employee | | |
| | Student | | |
| Date(s) of Contact: | | | |
| Method of Communication | | List email address/phone number used | |
| Email | | | |
| Text Message | | | |
| Telephone | | | |
| Other | (Please specify) | | |

| |
|---|
| <p>Details/Content of Electronic Communication (If possible, attach a copy of text of email, text, etc.)</p> <p>Act 214 of the 2009 Louisiana Legislative Session places limitations on electronic communications between students and teachers. As a general rule, all school employees should limit electronic communications with students concerning official school related activities. Contacting Students via social networking sites, such as Facebook, Twitter, and other social media, is not encouraged.</p> |
|---|

Turn in completed form to the school principal or building supervisor.

ST. MARTIN PARISH

EMPLOYEE TECHNOLOGY and INTERNET ACCEPTABLE USE POLICY

EMPLOYEE USER AGREEMENT

I have read the St. Martin Parish School District’s Employee Technology and Internet Acceptable Use Policy. I fully understand and agree to abide by this policy when utilizing the District’s computer equipment, network, or the Internet. I understand that any information, data, usage, files or electronic communications, including but not limited to email transmission, that I transmit via District’s systems, including but not limited to the Internet, may be monitored, accessed and reviewed by District Network Administrators, School Board’s Superintendent or designee. I further agree to instruct the students under my supervision on the acceptable and responsible use of the District’s computer equipment, network, and the Internet.

I understand that violation of this policy may constitute suspension and/or revocation of my device, network, and Internet privileges. I also understand that violation of this policy could result in **exclusion or termination of employment and/or civil or criminal liability under other applicable laws.**

Employee’s Name (PRINT): _____

Employee’s SIGNATURE: _____

School/Office: _____

Date: _____

Return this form to your supervisor, who is required to maintain a copy on file.