Children's Internet Protection Act (CIPA) - Compliance Policy

COMPUTER ACCESS AND USE

INTERNET SAFETY

In accordance with the *Children's Internet Protection Act (CIPA),* the **St Martin Parish Library** ("Board of Control") shall enforce a policy of Internet safety that incorporates the use of computer-related technology or the use of Internet service provider technology designed to block or filter Internet access to certain visual depictions, including without limitation those that are obscene, child pornography, or otherwise harmful to minors. Sites that are excessively, violent, pervasively vulgar, sexually harassing or that contain information regarding the manufacturing of bombs or other incendiary devices shall also be prohibited. Only authorized persons may disable the blocking or filtering mechanism *for an adult user* in order to enable Internet access for bona fide research or other lawful purposes.

In addition to filtering requirements, it shall be the policy of the **St. Martin Parish Library Board of Control** to:

1) Prohibit access by minors to inappropriate matter on the Internet and World Wide Web;

2) Institute measures to ensure the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications, such as "Instant Messaging";

3) Prohibit unauthorized access, including what is now known as hacking, and other unlawful on-line activities by minors online;

4) Prohibit unauthorized disclosure, use, and dissemination of personal information regarding minors; and

5) Institute measures designed to restrict minors' access to materials harmful to minors.

PERMISSIONS

1) The PROCEDURES AND POLICIES shall be made available upon request by any library patron and will be posted on the Library web site.

2) Library patrons permissions that are assumed include:

   · Access to the Internet and email system

   · Record of any site visited

COMPUTER AND INTERNET USE TERMS AND CONDITIONS

1) *Acceptable Use* - The purpose of the Internet is to support research and education in and among academic institutions in the United States by providing access to unique resources and opportunities for collaborative work. Transmission of any material in violation of any U.S., state, or local district regulations shall be prohibited.

2) *Netiquette* - Users shall be expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

· Be polite. Do not send abusive messages to others. Use appropriate language.

· Do not reveal personal addresses or phone numbers.

· Note that Electronic Mail (Email) is not guaranteed to be private. People who operate the system do have access to all mail. Messages related to or in support of illegal activities must be reported to the authorities. All users should be aware that routine monitoring of the system may lead to discovery that the user has or is violating the Acceptable Use Agreement.

· Do not use the network in a way that would disrupt the use of the network by other users (e.g. downloading huge files during prime time, sending mass email messages, or annoying other users using the talk or write functions). Hardware or software shall not be destroyed, modified, or abused in any way.

· Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system shall be prohibited.

· Hate mail, harassment, discriminatory remarks and other antisocial behaviors shall be prohibited on the network.

· The illegal installation of copyrighted software for use on computers shall be prohibited.

· Use of the network to access or process pornographic material, inappropriate text files, or files dangerous to the integrity of the local area network (LAN) shall be prohibited.

3) *Privileges* - The use of the Internet is a privilege, not a right, and inappropriate use shall result in a cancellation of those privileges and may result in disciplinary or legal action.

4) S*ecurity* - Security on any computer system is a high priority, especially when the system involves many users. Any suspected security problem on the Internet shall be reported to the Director, who shall immediately contact the Technology Coordinator. Any user

identified as a security risk or having a history of problems with other computer systems shall be denied access to the Internet.

5) *Vandalism* - Vandalism shall result in cancellation of privileges and or other disciplinary actions. *Vandalism* is defined as any malicious attempt to harm or destroy hardware or software data of the Library system, another user, the Internet Service Provider, or other networks that are connected to Internet. This includes, but is not limited to, the uploading or creation of computer viruses, "Digital Graffiti", defacing Websites, unauthorized changes to websites, programs, applications, databases, etc. No software, programs, or files may be installed or downloaded by any user.

6) *Consequences of Misuse* - Library user will be denied access to computers.

7) *Cyberbullying*: The State of Louisiana, Cyberbullying is defined in LA Rev Stat § 14:40.7 as is punishable under the law. The law defines Cyberbullying as,

> "the transmission of any electronic textual, visual, written, or oral communication with the malicious and willful intent to coerce, abuse, torment, or intimidate a person under the age of eighteen."

RESPONSIBLE USE / CODE OF CONDUCT

St. Martin Parish Library is a place of tolerance and good manners. Patrons may not use the network or computer facilities for hate mail, defamatory statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability.

***Code of Co*nduct** applies to all users of the Internet. Honesty, integrity, and respect for the rights of others should be evident at all times.

The use of the Internet, including the World Wide Web must be consistent with the objectives of the library. The **library** shall not be responsible for any financial obligations incurred by users of the Internet.

Cyberbullying shall result in cancellation of privileges and or other disciplinary action. Any validated reports of Cyberbullying which contains true threats of intent to harm a person, will be reported to law enforcement. The test of "intent to harm" is whether a reasonable person sending a communication would foresee that the listener would interpret the statement as a serious expression of intent to harm. Under LA Rev Stat § 14:40.7 persons convicted of Cyberbullying shall be fined not more than five hundred dollars, imprisoned not more than six months, or both.

The computer user shall be held responsible for his/her actions and activities. Unacceptable uses of the computers and/or the Internet shall result in appropriate disciplinary action, including

revoking of computer privileges. If a patron has questions about whether a specific activity is permitted, he or she should ask a library official.

If a patron accidentally accesses inappropriate material, he or she should back out of that information at once. Patrons who may inadvertently access a site that is pornographic, obscene, or harmful to minors shall immediately disconnect from the site.

Regulations for the use of computers and the participation by anyone on the Internet include but are not limited to, the following:

1) Library rules prohibiting cyberbullying, indecent, vulgar, lewd, slanderous, abusive, threatening, sexually harassing, or terrorizing language apply to all forms of electronic communications.

2) Patrons shall not post any e-mail or other messages or materials on library networks or the Internet that are indecent, vulgar, lewd, slanderous, abusive, threatening, sexually harassing, or terrorizing.

3) Patrons shall not access over the Internet visual depictions that are obscene, pornographic, or harmful to minors.

4) Patrons shall not attempt to gain unauthorized access, including so-called "hacking" or otherwise compromise any computer or network security or engage in any illegal activities on the Internet, including willfully introducing a computer virus, worm, or other harmful program to the network.

5) Patrons shall observe copyright law and fair use guidelines. Patrons shall not plagiarize or otherwise use copyrighted material without permission. Patrons shall properly cite the source of information accessed over the Internet.

6) Degrading or disrupting equipment or system performance shall not be permitted.

7) Invading the privacy of individuals, sending of hate mail, harassing, or making discriminatory remarks or other antisocial behavior shall be prohibited.

8) Using an account owned by another user shall be prohibited.

9) Posting anonymous messages shall not be permitted.

10) Perusing or otherwise accessing information on manufacturing bombs or other incendiary devices shall be forbidden.

11) Accessing or creating exposure in any way to pictures, graphics, or other visual depictions that taken as a whole and with respect to minors, appeals to the prurient interest in nudity, sex, or excretion shall be prohibited.

12) Accessing or creating exposure in any way to pictures, graphics, or other visual depictions that describe or represent in an 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 shall be prohibited.

13) Accessing or creating exposure in any way to pictures, graphics, or other visual depictions that taken as a whole lack serious literary, artistic, political, or scientific value as to minors shall be prohibited.

14) Use for product advertisement, political lobbying, or illegal activities shall be strictly prohibited.

CIPA MONITORING AND TRAINING

In addition to the use of technology protection measures, the monitoring of student's online activities and access to the Internet and World Wide Web may include, but shall not be limited to, the following:

1) Ensuring the presence of library personnel when patrons are accessing the Internet.

2) Provide annual training regarding CIPA policy to all library staff. Training will address key issues such as cyberbullying, social networking dangers and emerging technologies that may endanger patrons while using the Internet.

Revised August 2018

Ref: Ref: 47 USC Section 254 (Telecommunications Act), Pub. L. 106-554 (Children's Internet Protection Act), La. Rev. Stat. Ann. §17:81, 17:100.7, 17:280.