Webster Parish School Board
Internet Safety Plan

In compliance with state and federal regulations, the Webster Parish School Board utilizes CIPA (Children's Internet Protection Act) compliant filtering software and other technologies to prevent students from accessing websites including without limitation those that are obscene, pornographic, or harmful to minors, including without limitation sites that are excessively violent, pervasively vulgar, or sexually harassing. Sites which contain information on the manufacturing of bombs or other incendiary devices shall also be prohibited.

Compliance measures contained within this plan address the following areas:

Access By Minors To Inappropriate Matter On The Internet And World Wide Web

- Users shall not use the district Internet system to access material that is profane or obscene (pornographic), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). For students, special exception shall be made for hate literature if the purpose of such access is to conduct research AND both the teacher and the parent approve access. District employees shall access the above material only in the context of legitimate educational research.

- If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in a manner specified by their school. Students should immediately notify teachers. Teachers and staff should immediately notify building administration. Building administration should immediately notify the coordinator of technology. This shall protect users against an allegation that they have intentionally violated the *Acceptable Use Agreement*.

- Electronic access may include the potential for access to inappropriate content despite the best efforts of supervision and filtering because no content filtering is capable of blocking 100% of the material available on the Internet. The fact that the filtering technology has not protected against access to certain material shall not create the presumption that such material is appropriate for users to access.

- School staff is responsible for monitoring district personal computing device usage, district Internet system usage, work in progress, and online activities of minors while at school. Parents/guardians are responsible for monitoring the usage of district personal computing devices, district Internet systems, and access to information on the Internet while at home. Each student and his/her parent/guardian should be aware that the Webster Parish School Board does not have control of the information on the Internet, nor can it provide comprehensive barriers to students accessing information on the Internet. Sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate, illicit, or potentially offensive to some people. While the Webster Parish School Board makes efforts to filter objectionable content on district personal computing devices and district Internet systems both at school and at home, parents and guardians must remain diligent in observing student behavior when using these devices at home, including the sites visited by the student and communications to and from the student while using the devices. Should access to an inappropriate site occur, or should a student send or receive inappropriate content while using a district personal computing device or district Internet system, the student must notify their teacher or building level administrator immediately.

Safety and Security Of Minors When Using Electronic Mail, Chat Rooms, And Other Forms Of Direct Electronic Communications And Unauthorized Disclosures

- Student users shall not post or share contact information about themselves or other people. Personal contact information includes the student's name together with other information that would allow an individual to locate the student, including, but not limited to, parent(s) name(s), home address/ location, work address/location or phone number.

- Elementary school students shall not disclose their full name or any other personal contact information for any purpose.

- High school and middle school students shall not disclose personal contact information, except to education institutes for educational purposes, companies or other entities for career development purposes or with specific staff approval.

- Students shall not disclose names, personal contact information, or any other private or personal information about other students under any circumstances. Students shall not forward a message that was sent to them privately without permission of the person who sent them the message.

- Students shall not agree to meet someone they have met online.

- Students shall promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable. Students should not delete such messages until instructed to do so by a staff member.

Unauthorized Access, Including "Hacking" And Other Unlawful Activities By Minors Online

- Security on any computer network is a high priority, especially when the network involves many users. If a user feels he/she can identify a security problem on the computer network, the user must notify a building level administrator. The user should not inform individuals other than building level administrators of a security problem. The building level administrator shall report the security issue to the coordinator of technology.

- Users are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person other than the building level administrator or his/her designee.

- Passwords to the network should not be easily guessed by others nor should they be words that could be found in a dictionary.

- Attempts to log in to the network using either another user's accounts or as a network administrator could result in termination of the user's accounts. Users should immediately notify a building level administrator if a password is lost or stolen or if they have reason to believe that someone has obtained unauthorized access to their account. Any user identified as a security risk shall have limitations placed on usage of the network or shall be terminated as a user and be subject to other disciplinary or legal action.

- Users shall not attempt to gain unauthorized access to the district system or to any other computer system through the district system or go beyond their authorized access. This includes attempting to log in through another person's accounts or access to another person's files. These actions are illegal, even if only for the purpose of "browsing".

- Users shall not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.

- Users shall not use the district system to engage in any illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of another person, etc.

- Users shall not attempt to access web sites blocked by district policy, including the use of proxy anonymizers, software download sites, VPNs, or commercial web sites.

- Students shall not attempt to access non-instructional district systems, such as student information systems or business systems.

- Users shall not use sniffing or remote access technology to monitor the network or other user's activity.

- Users shall not use any wired or wireless network (including third party Internet service providers) with equipment brought from home. Example: The use of a home computer on the network or accessing the Internet from any device not owned by the district. Any exceptions must be approved by the building level administrator and the coordinator of technology.

- Users shall not use district equipment, network, or credentials to threaten employees, or cause a disruption to the educational program.

- Users shall not possess published or electronic material that is designed to promote or encourage illegal behavior or that could threaten school safety, nor use the Internet or Web sites at school to encourage illegal behavior or threaten school safety.

- Users shall not use the district equipment, network, or credentials to send or post electronic messages that are abusive, obscene, sexually oriented, threatening, harassing or damaging to another's reputation since these acts are illegal.

Technology Protection Measure (Internet Filtering) To Restrict Minors' Access To Materials Harmful To Minors

The Webster Parish School Board has selected a technology protection measure (Internet filtering) for use with the district Internet systems and district personal computing devices. The filtering technology shall be configured to protect against access to material that is obscene, illegal (i.e. child pornography) and material that is harmful to minors, as defined by the Children's Internet Protection Act (CIPA). The district and/or individual schools shall, from time to time, reconfigure the filtering software to best meet the educational needs of the district or schools and address the safety needs of the students.

The filter shall not be disabled at any time that students shall be using the district Internet system, if such disabling shall cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. The filter can be disabled during non-student use time for system administrative purposes.

If an administrator or teacher believes that a blocked site should be unblocked, a web site review can be submitted to the coordinator of technology. The coordinator of technology shall make a decision to unblock access to the site or shall delegate the decision to other district level administrators. A site that has been unblocked, together with the rationale for making the decision, shall be forwarded to the building level administrator.

Educating Minors

Each year, all Webster Parish Schools will provide a lesson educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness and response, and cell phone safety.