MCCOMB SCHOOL DISTRICT ACCEPTABLE USE POLICY

The following policy is written to promote positive and effective digital citizenship among students, faculty, and staff.

McComb School District is pleased to be able to offer its students, faculty, and staff access to its network and the Internet. Access will provide students, faculty, and staff the ability to explore thousands of files, libraries, databases, bulletin boards, and network resources in support of educational research.

Network

The District network includes wired and wireless computers and peripheral equipment, files and storage, email and Internet content. The District reserves the right to prioritize the use of, and access to, the network. All use of the network must support education and research and be consistent with the mission of the District. The network is property of the district and is subject to be monitored or audited at any time. Equipment used to access the district's network may also be subject to be monitored or audited at any time.

The education of minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyber bulling awareness and response shall be the responsibility of all members of the McComb School District's staff. The safety and security of minors will be maintained through the monitoring of appropriate use of online resources, email, chat rooms, and other forms of electronic communications.

Cyberbullying

Cyberbullying is defined as the use of electronic information and communication devices—such as email, cell phone and text messages, instant messaging, videos, defamatory personal Web sites and online personal polling sites—to willfully frighten or harm others. Examples of this behavior include but are not limited to:

- sending false, cruel, or vicious messages
- creating websites that have stories, pictures and jokes ridiculing others
- breaking into an email account and sending vicious or embarrassing materials to others
- engaging someone in electronic communication and tricking that person into revealing sensitive personal information and forwarding that information to others.

The MSD has adopted the following policies to address the abuse of electronic communication technologies:

1. Any MSD staff or student who uses a school-provided communication device (including a computer) or computer network (a) with the intent to intimidate, harass, or coerce another person, or (b) to use vulgar, obscene, profane, lewd, or lascivious language to communicate such harassment, or(c) to threaten an illegal or immoral act shall be subject to district/school disciplinary procedures.

2. Any MSD staff or student who uses a personal communication device on school grounds or at a school-related function (a) with the intent to intimidate, harass, or coerce another person, or (b) to use vulgar, obscene, profane, lewd, or lascivious language to communicate such harassment, or (c) to threaten an illegal or immoral act shall be subject to district/school disciplinary procedures.

Consequences for Violation
Any violation of these regulations may result in loss of computer-system privileges and may also result in appropriate disciplinary action, as determined by district/school administrators, or possible prosecution through the judicial system.

Reporting and Investigating
Students and staff are required to report to designated staff any incidents of cyberbullying about which they are aware. Reports may be made anonymously. Designated staff will investigate all reports, using any electronic communications records currently kept by the school division, and recommend the district's/school's next course of action.

Unacceptable network use by district students and staff includes but is NOT limited to:

- Downloading, installation and use of non-educational games, audio files, video files or other applications (including shareware or freeware)
- Non-approved software use is prohibited for staff and students.
- Websites that promote "social networking" are prohibited for students. Posting or publishing any information on the Internet or in any other publication that portrays McComb School District or its affiliates negatively is prohibited.
- Outside, non-district email systems are prohibited (i.e. Yahoo, Gmail, Hotmail, etc.)
- Attaching unauthorized or personally owned software or network equipment including, but not limited to, items such as routers, switches, or wireless access points to the district network without written approval from the Superintendent or his/her designee is prohibited. Any such equipment may be confiscated.
- Hacking, cracking, vandalizing, and/or the introduction of viruses to networks and information systems. Physical modification or defacing equipment is strictly prohibited.
- Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material

Cell Phone/Text Messaging

Cell phone possession/use by students on all McComb School District campuses must adhere to the individual school's policy.

Filtering and Monitoring

To the extent practical, Internet filtering software shall be used to block or filter access to inappropriate information on the Internet or on other forms of electronic communications. 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. Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision determined by the Superintendent or his/her designee. The district reserves the right to block any website it deems inappropriate.
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.

- Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content.
- FERPA (Family Educational Rights and Privacy Act of 1974) protects the privacy of student education records. There will be an agreement on file signed by all McComb School District employees stating that they will follow FERPA guidelines when accessing or releasing students' educational records.

Stolen, Missing or Damaged Equipment

Any laptop, tablet, related equipment or software that is discovered to be stolen, missing or damaged must be reported to the administrator/supervisor at the building at which the item(s) was checked out IMMEDIATELY. The User should submit a report of the relevant events as well as any relevant documentation. If the User is found to have been negligent for the theft, loss, or damage, that User will be assessed the repair or replacement fee of the equipment.

AUP Forms

Acceptable Use Policy (AUP) forms for staff, students and volunteers must be filled out **before** accessing network resources. By signing this form, you are declaring that all use of the system will be in support of education and research and consistent with the mission of the District.