CYBERSECURITY BEST PRACTICES

The Office of the State Auditor's (OSA) objective is to ensure that all school districts in the State of Mississippi are in compliance with the Children's Internet Protection Act (CIPA) and Family Educational Rights and Privacy Act (FEPRA) regulations and to ensure that every student is protected from accessing pornography and other explicit material that could be harmful while browsing the web on school issued devices.

With rapid changes in technology, it is critical to govern and monitor the activities of students while they access the Internet. OSA recommends all school districts strengthen their Technology Protection Measures (TPM) by ensuring controls are in place to properly block and filter devices used by students. OSA recommends districts create policies, but also implement those policies as well as train all administrative staff, teachers, students, and parents on the importance and danger of safe web browsing and the effects of improper online activity.

OSA intends to ensure that all students in the State of Mississippi are protected from harmful materials when browsing the Internet on school issued devices. Therefore, an effective mechanism to monitor online activities of students is critical and should be established, reviewed, tested, and fully implemented to make sure students are fully protected.

Parents and Students

- Notify administrative staff, teachers, parents, and students of the Internet Safety Policy or Acceptable Use Policy;
- Inform administrative staff, teachers, students, and parents about the Technology Protection Measures and ensure each individual understands the potential dangers of Internet browsing;
- Suggest to parents additional protections features that can be used within the home for additional filtering and monitoring;
- Continuously educate students about online safety and appropriate online viewing; and
- Provide community outreach within the district to inform parents on ways of keeping students safe while browsing the Internet.

District/Information Technology Staff

- Ensure the District has adopted the Internet Safety and Acceptable Use policies;
- Clearly define all elements of the policy to new employees and vendors;
- Review student's activities utilizing the TPM reporting features;
- Evaluate/test the efficiency of the District/Schools internet filtering measurements;
- Perform regular CIPA assessments on the network(s);
- Consider installing filtering software on computers and servers that can be effective offsite;
- IT staff should stay actively aware of proxy websites used to reach restricted sites;
- IT staff Statewide should share known proxy sites with other IT personnel;
- Implement internet safety protocols and post throughout the schools to communicate the importance of sensible web browsing and internet safety;
- For safe searching, all district issued devices should be set to "Safe Search" Mode;
- Restrict students from downloading and installing information that is not for educational needs; and
- Build a strong cybersecurity culture by performing regular security awareness education and training activities for all school employees (teachers, administrators, IT staff, etc.).

Please note, this best practices document may not contain all cybersecurity-related activities to adequately secure information technology infrastructure.