Smithville ISD Internet Safety Guidelines

1. Purpose

The purpose of the Internet Safety Guidelines document is to ensure that students and staff of Smithville ISD use technology resources, including the Internet and school networks, safely, responsibly, and in compliance with federal and state laws, including the Children's Internet Protection Act (CIPA). These guidelines are also, in compliance with board policy CQ (LEGAL) and CQ (LOCAL).

2. Scope

This policy applies to all students, staff, and users who access the SISD network, Internet, or digital resources using school-owned devices, networks, or platforms, whether on or off school property.

3. Definitions

- Inappropriate Content: Content that is obscene, pornographic, harmful to minors, or otherwise unsuitable in an educational setting.
- Cyberbullying: The use of digital devices to harass, intimidate, or bully others.
- Personal Information: Identifiable information such as full name, home address, phone number, Social Security number, or any other information that could be used to identify or locate an individual.

4. Internet Filtering and Monitoring

- The district shall employ filtering hardware and software to block access to content deemed inappropriate or harmful to minors.
- The district shall employ network and internet filtering software including firewalls, DNS, URL, category based and content filtering for malware, data breaches, and phishing.
- The district applies network and internet filtering to all network activity, including ethernet and Wifi-based traffic.
- The district shall employ filtering hardware and software to mitigate potential malware and ensure compliance with data protection policies.
- All network and internet activity will be monitored to ensure compliance with state and district policies.
- Network and internet filtering measures will not be disabled for staff or students.

5. Digital Citizenship and Education

Students will be educated on:

- Safe and responsible use of the Internet.
- Recognizing and avoiding cyberbullying.
- Protecting personal information online.
- Understanding copyright, plagiarism, and digital footprints.

6. Acceptable Use

Students and staff are expected to:

- Use the Internet and digital resources for educational purposes only.
- Communicate respectfully and responsibly.
- Refrain from accessing or distributing harmful or inappropriate material.
- Report any security problems or violations to a teacher or administrator.

7. Prohibited Activities

Users shall not:

- Attempt to bypass network or internet filters or access blocked content.
- Use school devices to access social media platforms not approved for educational use.
- Share personal information or the personal information of others.
- Engage in cyberbullying or online harassment.
- Download, install, or use unauthorized software or applications.

8. Data Privacy and Security

- The district will protect the confidentiality of student and staff data in accordance with FERPA, COPPA, and state privacy laws.
- Users are expected to use secure passwords and not share login credentials.

9. Enforcement and Consequences

Violations of this policy may result in:

- Suspension or revocation of technology access privileges.
- Disciplinary action per the student or employee handbook.
- Legal action if applicable.

10. Guideline Review

These guidelines will be reviewed annually and updated as needed to reflect current laws, technologies, and best practices.

Public Hearing Date: 4/21/25