Internet Safety Practices

Content Filtering and Internet Protections

1. Overview

Filtering inappropriate content is federally required under the Children's Internet Protection Act (CIPA). Schools and libraries subject to CIPA are required to adopt and implement an Internet safety practices addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them.

2. Purpose

The purpose of this document is to outline Montgomery County Public Schools' (MCPS) practices and procedures to filter internet content and to restrict students and staff from accessing inappropriate content while using MCPS internet services and devices. Internet services may include, but is not limited to: Wi-Fi access points, physical ethernet drops, mobile hotspots, and other internet services maintained by the district. Devices may include, but are not limited to: desktop computers, laptop computers, Chromebooks, Android tablets, and Apple devices.

3. Practices

MCPS utilizes industry standard Content Filtering services to filter out inappropriate web content in order to comply with CIPA. The vendors that provide these services maintain a list of categories that they use to classify websites. Based on these categories, MCPS blocks categories of websites with inappropriate content. If a website falls into a category that is blocked by MCPS, students and staff will be unable to access that website while using MCPS devices or Internet services as defined above. MCPS consistently blocks inappropriate content in order to provide safe instructional web content for students and staff. A blocked website may be unblocked if MCPS determines that the website is necessary for instruction or other educational or operational purposes.

Websites that are categorized into any of the following categories are blocked by MCPS:

Abortion	Freeware	Nudity/Risque
Alcohol	Gambling	Phishing
Child Abuse	Gaming (Non-Educational)	Plagiarism
Dating	Hacking	Pornography
Discrimination	Hunting	Proxy Avoidance
Drug Abuse	Illegal/Unethical	Social Networking
Dynamic DNS	Lingerie/Swimsuit	Spam URLs
Explicit Violence	Malicious Websites	Tobacco
Extremist Groups	Marijuana	Weapon Sales
File Sharing	Meaningless Content	Web Chat

4. Compliance

A. Compliance Measurement

The MCPS Office of the Chief Technology Officer verifies compliance with the above practices through various methods, including but not limited to: periodic website access attempts, end-user internet report auditing, business tool reports, and internal and external audits.

B. Exceptions

A school principal, a site supervisor, or a director may submit a request to the MCPS Help Desk to unblock a website. A request to unblock a website will be granted upon written approval by the Deputy Superintendent of Schools or the deputy's respective designee.

C. Non-Compliance

A student or staff member found to be intentionally circumventing the content filter and internet safeguards established by MCPS will be found in violation with Regulation IGT-RA, *User Responsibilities for Computer Systems, Electronic Information, and Network Security*.

5. Revision History

This document was revised on March 23, 2020.
This document was created on January 10, 2020.