7104 Internet Content Filtering

1. Purpose
    a. In an effort to protect our students, staff, and network resources from potentially harmful internet content, as well as to meet the requirements of the Children's Internet Protection Act (CIPA), Karl G Maeser Preparatory Academy will employ technology based solutions to filter all internet access originating from the school's network. This policy outlines inappropriate content, establishes a mechanism to address new content filtering requirements, and establishes responsibility for enforcement.
2. Filtered Content
    a. CIPA mandated content filters will be enforced, including a restriction on pornographic content, obscene content, violence, and other websites that are potentially harmful to children. Additionally, any content that carries a significant threat to network security or performance may be filtered.
3. Filtered Categories
    a. Filtered content lists are maintained within the school's internet content filtering device. Most filtered content is filtered automatically, based on frequently updated category definitions provided by the content filter vendor. Additionally the G Suite Management Console adds another layer of security via Safe Search and customized settings. This allows fine tuning of restricted sites and apps such as YouTube. These are global policies, applied to all students. Blocked categories include:
        i. pornography,
        ii. botnets,
        iii. confirmed spam sources,
        iv. dating,
        v. drugs,
        vi. keyloggers and monitoring,
        vii. malware sites,
        viii. nudity,
        ix. online gambling,
        x. proxies,
        xi. pay to surf,
        xii. peer to peer,
        xiii. phishing and other frauds,
        xiv. proxy avoidance and anonymizers,
        xv. spam urls,
        xvi. spyware and adware, and
        xvii. unconfirmed spam sources
    b. Content that matches the filtered categories but that is not caught by our automatic filter will be added to an explicit block list at the discretion of the director of technology.
4. Block and Allow Requests
    a. Occasionally there will be a reason to filter internet content that does not match one of the categories listed above, or there may be a reason to

allow a site that is blocked. Requests to block or unblock sites or services should be submitted to the technology department. In conjunction with Administration, the director of technology will consult to determine if blocking or unblocking the resource matches school policy and will then determine if a request should be granted or not. In an urgent situation, the director of technology may immediately deny a request if Administration is unavailable and the request does not meet the standards of the school policy.

5. Resources
    a. Digital citizenship and internet safety education will be provided to new students, staff, and parents. Online resources and in person training are available as needed.
6. Enforcement
    a. Internet content filtering policies are enforced by the technology department and school administration. This is in accordance with operations policy 2103 “Acceptable Use Policy”.

Approved October 13, 2020