مـــدرســـة الـشـــارقـــة الأمريـكـيـة الـدولـيـة
Sharjah American International School

SHARJAH AMERICAN INTERNATIONAL SCHOOL – UMM AL QUWAIN

Internet Use Monitoring and Filtering Policy

1. Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within SAIS's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner and ensure that employee web use can be monitored or researched during an incident.

2. Scope

This policy applies to all SAIS employees, contractors, vendors and agents with a SAIS -owned or personally owned computer or workstation connected to the SAIS network.
This policy applies to all end user-initiated communications between SAIS's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

3. Policy

3.1 Web Site Monitoring

The Information Technology Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

3.2 Access to Web Site Monitoring Reports

General trending and activity reports will be made available to any employee as needed upon request to the Information Technology Department. Computer Security Incident Response Team (CSIRT) members (Mr. Kumar) may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CSIRT upon written or email request to Information Systems from a Human Resources Representative.

3.3 Internet Use Filtering System

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for SAIS's corporate environment. The following protocols and categories of websites should be blocked:

- Social Network Services
- Personals and Dating
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email
- Peer to Peer File Sharing

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear

3.4 Internet Use Filtering Rule Changes

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules. The administration shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

3.5 Internet Use Filtering Exceptions

If a site is mis-categorized, employees may request the site be unblocked by submitting a ticket to the school principal. The principal will review the request and request to unblock the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for education purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a written request to the school principal. The principal will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

4. Policy Compliance

5.1 Compliance Measurement

CSIRT (Kumar) will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits.

5.2 Exceptions

Any exception to the policy must be approved by the school principal.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

I have read, understand, and will abide by the above Policy. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be initiated, as following:

1st Occurrence: Verbal warning / Written Warning is issued depending on the violation degree

2nd Occurrence: Final Written warning is issued, the staff member signs an undertaking.

3rd Occurrence: Dismissal from SAIS

Username: ……...

User Signature: ……

Date: ……

This policy was reviewed in August 2021.