INDIAN SCHOOL RAS AL KHAIMAH, UAE

SCHOOL POLICIES –
INTERNET FILTERING POLICY 2022-23

DECEMBER 2018
REVIEW AUGUST 1,2020
NEXT REVIEW MARCH 2021
REVIEWED ON MAY 2022
NEXT REVIEW ON MAY 2023

Internet Filtering Policy

Everyone at Indian School RAK takes internet use and the associated safety of our students extremely seriously.

However, it is essential to note that any filtering service can never be comprehensive, no matter how thorough. Schools must have a clearly understood policy on acceptable use for all users and maintain adequate supervision.

If school staff or students find themselves able to access internet sites from within the school that they think should be blocked, they should advise the school Principal (or, in his absence, the IT Coordinator). The Principal should report the matter to **the police/cyber crime department** if any ecrime/incident has been reported.

. All actions should be taken immediately.

Two Systems

In Indian School RAK, internet access has been done through two methods:

1. Internet access through WIFI.
2. Internet access through LAN.

Internet access through WIFI

Schools provide WIFI access to teachers, staff, visitors and students. Teachers and staff are allowed to bring their own devices on required occasions, where BYOD Policy will be accountable. Different level of users has been categorised School has implemented an effective firewall system, as a result of which the following categories of websites are not, by default, available to schools: -

- **Adult**: content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity;
- **Violence**: content containing graphically violent images, video or text;
- **Hate Material**: content which promotes violence or attack on individuals or institutions based on religious, racial or gender grounds;
- **Illegal drug taking and the promotion of illegal drug use**: content relating to the use or promotion of illicit drugs or misuse of prescription drugs;
- **Criminal skill/activity**: content relating to the promotion of criminal and other activities;

- **Gambling**: content relating to online gambling websites or information relating to the promotion of gambling and gambling advice.

It defines three types of access:

- **GREEN** – accessible to all users in schools;
- **AMBER** – accessible to schools' selected groups of users
- **RED** – not accessible to any user.

This filtering policy is managed by IT Department.

Internet access through LAN

The School IT Infrastructure, including computer labs, office systems, interactive panels etc., is connected through LAN, which will also pass through our firewall system, so the above filtering policy is applicable for devices attached through LAN.

Summary

The school's wifi and IT infrastructure have been installed. They are maintained with an active, monitored filter system to satisfy both the needs of child protection/inappropriate content whilst ensuring that it serves to support teaching and learning.

Access to network

Access to the WIFI network is provided through password authentication using WPA. There will be two-level of authentication to join the wifi network. After making password authentication, users must log in using ID and password based on which category they belong to, whether teachers, leaders, staff, etc. A wifi controller has been set up for this. This key is not available to any staff aside from the school. Visitors will be given limited access with a login if that is required. Therefore, access is governed by unique user registration and monitored by the IT coordinator. No devices can join the network without this login and authentication.

Hardware and general service provision

The following has been installed and configured in the school to ensure only appropriate content is available to all users:

1. A hardware firewall filter is installed, which intercepts all Internet traffic leaving and entering the school network, which cannot be circumvented. The Sophos firewall appliance is configured for the Internet filtering service. This service is a professional; commercial category-based web filtering solution is used worldwide. It uses a category based system to group websites in addition to the keyword, IP and specific white and blocklist control. School licenses are purchased on a fixed three-year term to ensure continuity of service, and the individual firewall is monitored 24/7 with instant notification of any concerns.

2. In addition, IP and URL black and whitelisting are supported locally, which ensures any content that is flagged as non-desirable on the network can be disabled immediately

3. Full access logs are maintained for all traffic and attempts to access inappropriate content.

Specifics of filtering service

This filtration service uses a category based system to decide if a website is viewable from all Internet-connected devices. The primary Categories include:

- Child Protection (including violence, porn, weapons etc.)
- Leisure (entertainment, travel, sports)
- Business
- Chatting (internet chatting and instant messaging services)
- Computer & Internet Services (social networking, streaming, spam sites)
- Other (image sharing, dating and person, compromised, etc.)

If a website falls into a category that is not deemed acceptable for use in the classroom. The user will be subject to viewing an “unsuitable” notification on the web browser, and this activity will be logged to the user and device level.

Additional filtering

To supplement category-based filtering, the school maintains a rolling list of websites requested by teaching staff, checked and approved to be exempt from category filtering, and this is available in school. This list is maintained by the IT Coordinator and relevant eSafety coordinator. Websites are added to a specific blocking list where required.

School Procedures

The school has a mechanism should a website be uncategorised and can request a category to be allocated from within the URL category tool.

Individual websites can be permitted through the filtering system on a site per-site basis using White Listing. This is particularly useful when blocking such apps as Twitter, Facebook and Tiktok that operate within an 'App' environment.

Further Notes

- Filtering has been checked by two senior staff.
- Two staff members have been trained in filter use to react with speed to any system issue.
- The school’s eSafety policy has been changed to match these changes and systems.

This policy was compiled in October 2018 and is subject to review and update.The policy was reviewed in Mar 2022.