FILTERING POLICY

2023-2024

المدرسة الهندية العالمية الخاصة
INTERNATIONAL INDIAN SCHOOL

Reviewed & Updated: April 2023
Next review : April 2024
Prepared by School Council Members

Members of the committee

- Mr. Wasim Yousuf Bhat (Dean)
- Mr. Qurat al Ain (Principal)
- Mr. Mujeeb Rahman (Administrative Officer)
- Ms. Reshma A (Software Analyst)
- Mr. Boney R (IT Administrator- Corporate)
- Mr. Sabeel K (IT Administrator- School)
- Mr. Jayakrishnan (Section Head Grade 6-12-Boys)

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Scope

This policy applies to all anyone accessing the Internet on devices that are connected to the School name network, including School owned, personally owned, and mobile devices.

Responsibilities

This policy applies to all anyone accessing the Internet on devices that are connected to the School name network, including School owned, personally owned, and mobile devices.

The responsibility for the management of the school's filtering policy will be held by IT ADMINISTRATOR. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- be logged in change control logs
- be reported to IT administrator
- be reported to and authorized by IT administrator prior to changes being made
- be reported to the Online Safety Group every 6 months in the form of an audit of the change control logs

All users have a responsibility to report immediately to IT ADMINISTRATOR any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmers or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customized filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider – As per UAE TRA (Telecommunications Regulatory Authority)
- The school manages its own filtering service
- The school has provided enhanced/differentiated user-level filtering through the use of the filtering programme. (Allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal (or other nominated senior leader).
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.

  Requests from staff for sites to be removed from the filtered list will be considered by the IT ADMINISTRATOR. The IT ADMINISTRATOR, in conjunction with the online safety group, will periodically review and recommend changes to Internet filtering rules. Senior Leadership shall review these recommendations and decide if any changes are to be made.

Education/Training/Awareness

Pupils/students will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

the Acceptable Use Agreement

Induction training

Staff meetings, briefings.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions/newsletter etc.

Changes to the Filtering System

If a website is blocked, employees should consult with their manager before requesting an exception. Managers may submit a request to review a blocked website by contacting the International Indian IT Administrator. The Network Admin will review the request, will communicate updates to the employee and Manager, and will consult with vendors, as well as the School Online Safety team, as needed.

- If the Network LAN Admins determine a website is properly categorized per our security systems, the security team shall be consulted to decide if changes are to be made, such as unblocking the website, if proper business justification has been documented by the employee and manager.
- If the site is confirmed to be mis-categorized, the Network LAN Admins may unblock the site until the necessary changes are released by the vendors.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to IT ADMINISTRATOR who will decide whether to make school level changes.

All categories other than below mentioned are blocked in School network.

- Arts and culture
- Education
- Health and wellness
- News and media
- Sports
- Information and computer security
- Information technology
- Online meeting

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. Monitoring will take place as follows:

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:
IT Administrator
Online Safety Group
External Filtering provider

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

School IT dept. provides an effective filtering 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 on the basis of religious, racial or gender grounds;
- **Illegal drug taking and the promotion of illegal drug use**: content relating to the use or promotion of illegal drugs or misuse of prescription drugs;
- **Criminal skill/activity**: content relating to the promotion of criminal and other activities;
- **Gambling**: content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.

Access to network:

Access to the network is provided through password authentication using WPA. This key is not available to any staff aside from the school. Access is therefore governed by unique device registration and pre-approval.

Hardware and general service provision:

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

A hardware firewall filter is installed which intercepts all Internet traffic leaving and entering the school network and this cannot be circumvented. This firewall appliance is configured for the Global view Internet filtering service. This service is a professional, commercial category based web filtering solution in use. It uses a category based system to group web sites in addition to keyword, content filtering, IP and specific white and blacklist 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.

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

Full access logs are maintained for all traffic and all attempts at access of inappropriate content.

Enforcement

The Network Admins and the School Online safety team will periodically review Internet use filtering systems and processes to ensure they are in compliance with this policy.