المدرسة الهندية النموذجية الجديدة

NEW INDIAN MODEL SCHOOL

Internet Safety Policy for Infrastructure

The New Indian Model School, Sharjah employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor students' Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal floppy disks, memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

World Wide Web

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will report accidental accessing of inappropriate materials in accordance with school procedures.
- Students will use the Internet for educational purposes only.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students will never disclose or publicise personal information.
- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.
- Students will use approved class email accounts under supervision by or permission from a teacher.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.

- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.

School Website

- Students will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of students or staff.
- The publication of student work will be coordinated by a teacher.
- Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs, audio or video clips of focusing on group activities. Content focusing on individual students will not be published on the school website without the parental permission. Photographs, audio and video clips will focus on group activities. Video clips may be password protected.
- Personal student information including home address and contact details will be omitted from school web pages.
- Students will continue to own the copyright on any work published.

Internet Access in Campus

- Students will be allowed to access the internet on the *lab computers* or on their *personal devices* under supervision of the respective teacher. Student networks will be strictly restricted by web content filters in firewall and are allowed to access only educational contents.
- Academic staff are allowed to use their personal devices, and will have access to limited internet contents with fewer restrictions. Staff will take permission from the management prior to usage, and the IT administrator will register the MAC address of the device to give access to the network.
- Administration staff will have access to the internet as well as the internal network.

List of allowed contents are decided by the school management and are reviewed regularly. Requests to access specific contents will be submitted to management with proper justification. The IT administrator will then review the contents to ensure the authenticity and safety of the content. After getting approval from the management, the IT administrator will make the necessary changes in the web filtering rules.

Personal Devices

BYOD policy of school encourages students and staff to bring their personal devices to campus for learning purposes. However, students using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving is in direct breach of the school's acceptable use policy.

3. School Network Infrastructure Design

Introduction

This document provides best practices to schools to better manage student access to Internet content and improve the IT security posture to match the adoption of classroom student computers. The target audience is IT infrastructure planners and network designers. This network architecture describes a network design tailored for mobile, Wi-Fi network, student computers.

Overview

The basic network infrastructure components starting from the edge of the network to the Internet
connection are:

1. **WiFi access point** (also called wireless router, AP, or WAP). This device advertises the school's wireless networks and enforces the first level of network access policy. Access points are typically located in the classrooms and distributed in a manner so adjacent access points can automatically detect and serve the computer in the event of an access point loss.
2. **The LAN switch** is a device located in the room where the network cabling terminates is a major starting point for troubleshooting reports of network slowdowns. The switch provides multiple Ethernet ports or interfaces to both hard wired and wireless access points. The switch plays a critical role in forwarding network traffic among access points, hard wired devices, firewall, and content filter. One of the key roles is distributing Virtual Local Area Network (VLAN) access.
3. **The firewall** and **Web content filter** (also called security appliance) are often combined with the network routing. The more complex Internet access policies are maintained here. This is often one of the primary control points for enforcing the school's Child Information Protection Act (CIPA) policy. Differential policies for social network access for students v. staff are maintained here. The school's Internet modem is directly connected to the security appliance and in turn the security appliance connects to the LAN switch. This is the central location for network routing between Virtual Local Area Networks (VLANs) LAN switch.

School Network Design

Wifi Access Points

School provides campus-wide access to wireless internet through a centralized wifi system that consist of a Unifi Wireless Access Controller and Unifi WAPs from Ubiquiti

Access to wireless networks is controlled by MAC address filtering in the firewall. Any user who requires access should get permission from the school management, and then contact the IT administrator. The user's device MAC address is then collected and added to the appropriate allowed list in the firewall.

Configurations include

- ***Bandwidth management:*** to ensure the overall internet bandwidth is equally distributed among all devices to ensure the smooth connectivity.
- ***Segmented network***: separates the student network from the administration network, ensuring more security.
- ***Roaming***: users can roam around the campus without disconnection. Wireless controllers effectively handover the connection from one access point to another.

Local Area Network

Campus network is segmented into multiple Virtual LANs according to the following levels of access rights. Infrastructure is managed by CISCO switches and pfSense Firewall.

1. ***Administration VLAN* :** accessible to administration staff via wired and wireless network. They have access to Internet access as well as critical internal resources such as the shared storage drives, access to sensitive data.
2. ***Teacher VLAN*:** accessible to academic staff with access to the internet with limited access.
3. ***Student VLAN:*** accessible to all students on their personal devices which are permitted by the management to use inside campus. They have access to the internet with restricted access to contents according to the policy set by the school management.

Network devices are physically secured in cabinets with access only given to the IT administrator. Protection of devices and the equipment rooms are ensured by the building security.

Firewall

School network Infrastructure is guarded by Unified Threat Management Solution based on pfSense platform. It integrates the following security services in a single appliance.

- Firewall
- URL filtering
- Web content filtering (pfblockerNG)
- Virtual private networking
- DHCP

Event Log Management

Event log analyzer software implemented in school is configured to collect the syslog information from network devices like firewalls and switches, to generate reports on demand. IT administrators review these reports regularly to ensure the availability of IT services. These logs are used for monitoring, reporting, and managing incidents.