I.T CONTENT FILTERING POLICY

Approved by:	Head Teacher	**Date:** 02.09.2021
Last reviewed on:	06 September 2021	I.T Dept (Irfan)
Next review due by:	September 2022	

Al-Khair School's - Internet Content Filter Policy

At Al-Khair School, we take content filtering extremely seriously, ensuring no staff or students are exposed to inappropriate content while on any of its premises.

We have 3 systems in place, which this document sets out to explain:

1. Draytek - GlobalView Content Filtering
2. OpenDNS – FamilyShield
3. Google – "SafeSearch On"
4. Monitoring & Mobile Devices & BYOD

1. Draytek - GlobalView Content Filtering

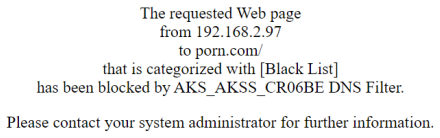
Draytek GlobalView Content Filtering (Cyren Powered) in place.

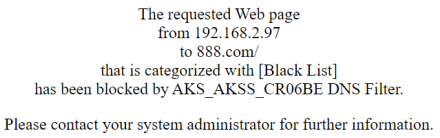
This is a service that constantly evaluates a websites category, adding it onto its database into a specifically defined and worldwide recognised category system.

Our firewall has been configured to filter out the following categories, which come under Cyren's Child Protection Category and a few others:

Alcohol & Tobacco
Criminal Activity
Gambling
Hate & Intolerance
Illegal Drug
Nudity
Porn & Sexually
Violence Weapons
School Cheating
Sex Education
Tasteless
Child Abuse Images
Anonymizers
Forums & Newsgroups
Download Sites
Streaming, Downloads
Phishing & Fraud
Social Networking
Spam Sites
Malware
Botnets
Hacking
Illegal Software
Peer-to-Peer
Cults

This is implemented at the root level, directly on our firewall, meaning weather a user is connected via Wireless or connected to a physical network port, all the above-mentioned categories will be blocked and unavailable to staff/students while connected to our network.





Last Test Date: **Monday 6th September 2021 – To be reviewed December 2021**

The above images show the message presented to anyone when trying to access any blocked categorised sites.

Further details are available here: https://www.draytek.co.uk/products/accessories/web-content-filtering

2. OpenDNS – FamilyShield

In addition to this, the network has been configured with OpenDNS "FamilyShield" in place at a Network DNS level for filtering.

"FamilyShield" is a special service offered by OpenDNS, meant for users who want to block inappropriate websites.

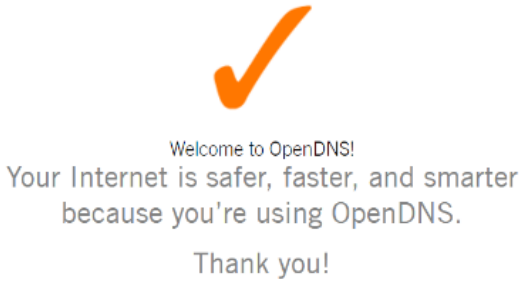
"FamilyShield" will always block domains that are categorized in their system as:

Tasteless
Proxy/Anonymizer
Sexuality
Pornography

Like the above Draytek system, this is implemented at the route level of the firewall as well.

Further information is available here:
https://support.opendns.com/hc/en-us/articles/227988047-Web-Content-Filtering-and-Security

This can be tested at anytime by visiting the following site: https://welcome.opendns.com/



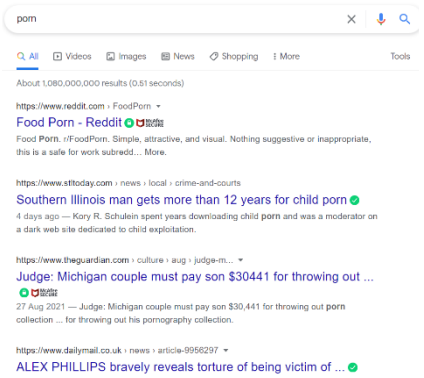
Last Test Date: **Monday 6th September 2021 – To be reviewed December 2021**

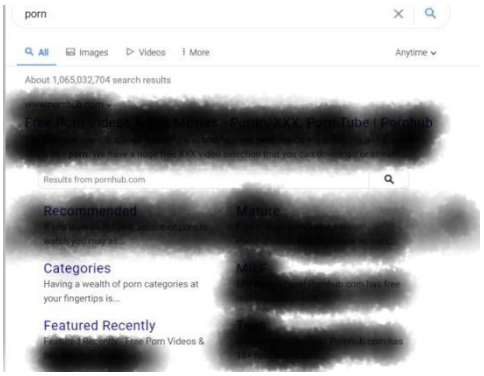
3. Google – "SafeSearch On"

Google's SafeSearch, helps filter out explicit content in search results for all your queries across images, videos, and websites. It's designed to help block explicit results from your search results. Explicit results include sexually explicit content like pornography, violence, and gore.

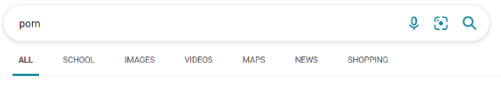
When a user uses Google or any other search engine to search for inappropriate content, this will filter out websites that are associated with that. Similarly, if the user tries to view images or videos, this is also blocked from displaying inappropriate results via Google, via Yahoo and Bing.

1. Search result when searching with the keyword "porn"

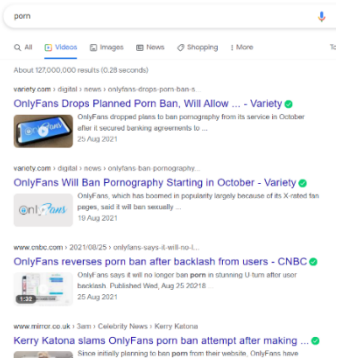


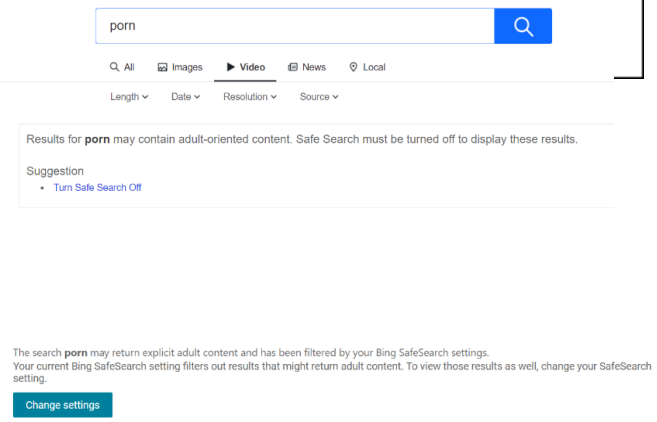


2. Search results when trying to access videos

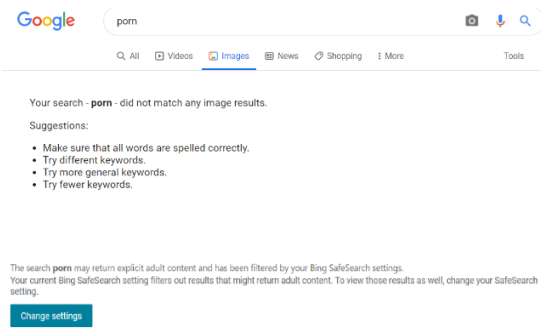


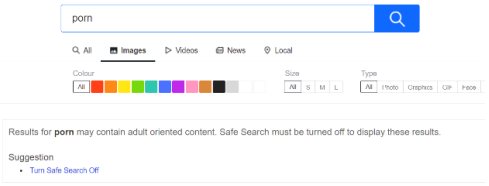
While textual search results are shown via Yahoo Search, once links are clicked, they are blocked by the Draytek Global Content Filter and the relevant messages appear.





3. Search results when trying to access images





Last Test Date: **Monday 6th September 2021 – To be reviewed December 2021**

As all our content filtering systems are on the root network, other devices such as iPads and even staff pcs/laptops (including personal ones) have the same prohibitions.

4. Monitoring

As per the current KCSIE_2021_September guidelines, (like previous) there is a heavy emphasis on the filtering and safeguarding of children being able to access content deemed inappropriate.

We believe this criterion is being met with the above 3 mentioned content filtering applications.

We have therefore, opted for a Physical Monitoring approach with some low-level logging which can be used to investigate if logs are demonstrating worrying behaviour.

Access to student laptops is limited to a classroom setting. Whilst in use, teachers monitor online activities, and it is school policy to never leave students unsupervised in any classrooms.

Laptops are mainly used for ICT and Art lessons, with a handful of other disciplines using ICT occasionally.

iPads are only currently being used by Arabic teachers and these are managed by the teacher using “Apple Classroom”. This application allows teachers to see which applications a student is on and has the ability for a teacher to see the actual screen view of each iPad.

As the class sizes are very small with a maximum number of 20 students, we believe that this is a manageable and balanced approach of meeting the requirements vs cost benefit as outlined in Paragraph 128 KCSIE_2021_September guidelines.

A log is kept when the content management system is breached, however this is not attributed to any user, the device can be identified and if required further investigation can try and see how many breaches, times of day and liaising with school admin, can ascertain which class was responsible and question students/staff accordingly. Breaches are emailed and monitored by the IT department, and they will liaise with school admins/safeguarding staff if required.

Similarly, in the primary school, the ICT Lab has been setup so that all the monitors are inward facing, allowing the teacher to be able to view all screens with a single glance.

Mobile Devices & BYOD

There is a school policy for all students to hand their mobiles into form tutors every morning and available for collection at the end of the day. Students who fail to hand devices are reprimanded with parents being informed and phones confiscated.

There is no Wi-Fi access for students to use, with the main network only for staff devices and guest network passwords provided on a “need to know basis” and regularly changed.

The Wi-Fi system can block devices, these are reviewed regularly to ensure that all devices are school issued Computers, Laptops, iPads or staff laptops/mobile devices which have been authorised to use and connect to the network.