

This document outlines the web filtering categories on a FortiGate firewall for schools that haven't yet received their Managed Network Upgrade.

N4L's Web Filtering is fully funded as part of your Managed Network connection and is one of the tools available to help create a safer online environment for your students and staff. Our filtering can block website categories, individual websites and apps, but not specific content within a website. For example, YouTube is widely used to support learning. Schools can currently either allow YouTube, or block all access to it - it cannot filter out individual YouTube videos.

Our Web Filtering should always be used in conjunction with your school's own digital citizenship policy and acceptable use procedures. It's also important to remember that no filtering system is able to provide 100% protection from inappropriate content.

Recommended blocked categories

Websites categorised below are blocked as part of our Internet Safety & Security Services (previously known as Safe & Secure Internet) recommended settings. To unblock any of these will require the school to go through an opt-out process. In addition to these categories, schools can also ask us to block individual websites.

Child Abuse

Websites that have been verified by the [Internet Watch Foundation](#) to contain or distribute images of non-adult children that are depicted in a state of abuse.

Illegal or Unethical

Websites that feature information, methods, or instructions on fraudulent actions or unlawful conduct (non-violent) such as scams, counterfeiting, tax evasion, petty theft, blackmail, etc.

Crypto Mining

Websites that provide Crypto Mining tools, Mining pools, pooling of resources by miners, who share their processing power over a network.

Spam URLs

Websites or webpages whose URLs are found in spam emails. These webpages often advertise sex websites, fraudulent wares, and other potentially offensive materials.

Discrimination

Websites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.

Other Adult Materials

Mature content websites (18+ years and over) that feature or promote sexuality, strip clubs, sex shops, etc. excluding sex education, without the intent to sexually arouse.

Explicit Violence

This category includes websites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc.

Peer-to-peer File Sharing

Websites that allow users to share files and data storage between each other through services such as BitTorrent.

Drug Abuse

Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc.

Phishing

Counterfeit webpages that duplicate legitimate business webpages for the purpose of eliciting financial, personal or other private information from the users.

Proxy Avoidance

Websites that provide information or tools on how to bypass internet access controls and browse the web anonymously, includes anonymous proxy servers - which are sometimes referred to as VPNs (Virtual Private Networks). For example, Express VPN, Hot Spot Shield.

Potentially Unwanted Program

Sites using technologies that alter the operation of a user's hardware, software or network in ways that diminish control over the user experience, privacy or the collection and distribution of personal information, includes adware, spyware, browser hijackers, unwanted pop-ups and typo-squatting domains.

Hacking

Websites that depict illicit activities surrounding the unauthorised modification or access to programs, computers, equipment and websites.

Pornography

Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite.

Malicious Websites

Websites that host software that collects information and monitors user activity, and those infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus.

Terrorism

Websites containing content depicting terrorism-related acts which are, or appear to be, illegal in the jurisdiction of the originator of the rating, or sites which illegally incite the recruitment of individuals into terrorist organisations.

Extremist Groups

Websites that feature radical militia groups or movements with aggressive anti government convictions or beliefs.

Additional categories

Below are additional categories that your school can choose to block. The description for each of these categories can be found [here](#).

Suggested blocked categories - categories N4L strongly suggests blocking

Alcohol
Dating
Domain Parking
Dynamic DNS
Gambling
Lingerie and swimsuit
Marijuana
Meaningless Content
Newly Registered Domain
Nudity and Risque
Tobacco
Weapons (Sales)

Optional blocked categories - categories that are up to you to block at your own discretion

Abortion
Alternative Beliefs
File Sharing and Storage
Freeware and Software Downloads
Games
Instant Messaging
Newly Observed Domain
Remote Access
Search Engines and Portals
Sex Education
Social Networking
Sports Hunting and War Games
Web Chat
Web-based Email

Other categories - categories you can choose to block, but you shouldn't need to

Advertising	Education	Restaurant and Dining	Secure Websites
Advocacy Organisations	Job Search	Search Engines and Portals	Shopping
Armed Forces	Medicine	Entertainment	Society and Lifestyles
Arts and Culture	News and Media	File Sharing and Storage	Sports
Auction	Newsgroups and Message Boards	Folklore	Streaming Media and Download
Brokerage and Trading	Online Meeting	General Organisations	Travel
Business	Personal Privacy	Global Religion	Web Analytics
Charitable Organisations	Personal Vehicles	Government and Legal Organisations	Web Hosting
Child Education	Personal Websites and Blogs	Health & Wellness	Web-based Applications
Content Servers	Political Organisations	Information and Computer Security	
Digital Postcards	Real Estate	Internet Radio and TV	
Dynamic Content	Reference	Internet Telephony	

Recommended allowed search engine websites

The websites listed below are allowed by N4L due to their safe search functionality or content restrictions. **All other known search engines will be blocked** for schools under N4L's DNS Threat Protection service, or for schools that have selected to have the block applied.

- Google
- Bing
- safe.duckduckgo.com

Nearly 99% of searches on the Managed Network are conducted through Google and Bing. Google and Bing can both enable SafeSearch which filters the majority of inappropriate images and searches, and N4L can enforce this setting for schools and kura that use DNS Threat Protection.

Additional website and app safety blocks

N4L blocks access to the Grok AI platform (including the grok.com website and app) by default for schools that have opted in to Internet Safety & Security Services compliance monitoring.

Similar websites that provide the ability to generate inappropriate images are categorised as 'Adult' content and blocked as part of Internet Safety & Security Services recommended settings, and this precaution helps address the risks associated with the platform's ability to generate these unfiltered images and content.

If you would like to block any of these categories or specific websites for your school or kura, please call our Customer Support team on 0800 532 764 or email support@n4l.co.nz.

