

We're making your online learning environment safer



To help ensure your school's online learning environment is as safe as possible, we recommend blocking the default categories below. This further strengthens your school's protection against online threats (such as malware, phishing scams and VPN use), and helps restrict access to inappropriate content.

CATEGORY	DESCRIPTION (FORTINET)
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. Information on the Internet Watch Foundation is available at http://www.iwf.org.uk/
Discrimination	Websites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group
Drug Abuse	Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc.
Explicit Violence	This category includes websites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc.
Extremist Groups	Websites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs
Hacking	Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites
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.
Proxy Avoidance	Websites that provide information or tools on how to bypass Internet access controls and browse the Web anonymously, includes anonymous proxy servers
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
Pornography	Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite
Peer-to-peer File Sharing	Websites that allow users to share files and data storage between each other
Malicious Websites	Websites that host software that is covertly downloaded to a user's machine to collect information and monitor user activity, and websites that are infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus or trojan horse
Phishing	Counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users
Spam URLs	Websites or web pages whose URLs are found in spam emails. These web pages often advertise sex websites, fraudulent wares, and other potentially offensive materials