Appropriate Filtering for Education Settings

Sep 2025

Filtering Provider Checklist Responses

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self-review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] risks from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools, and FE) how their particular technology system(s) meet the nationally defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Palo Alto Networks
Address	22 Bishopsgate London
Contact details	Keir Williams & Hongbing Luo
Filtering System	NGFW - STRATA Firewall
Date of assessment	10/09/2025

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist, the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question, the appropriate self-certification colour for that question is AMBER.	

.

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
• Are IWF members		Palo Alto Networks is one of the highest contributors to the IWF, and we work in constant collaboration with the IWF and other agencies across the UK and around the world to help make the Internet a safer place for children. https://www.iwf.org.uk/membership/our-members/
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list), including the frequency of URL list updates		Palo Alto Networks' URL filtering solution is required to block all IWF-listed Illegal Child Abuse Images and all other Illegal content. Our solution takes a direct feed from the IWF URL block list. https://www.iwf.org.uk/membership/benefits-of-membership/
• Integrate the 'police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Palo Alto Networks' URL filtering solution actively integrates with the police assessed list of unlawful terrorist content produced by the Home Office and the counterterrorism referral unit.
• Confirm that filters for illegal content cannot be disabled by anyone at the school (including any system administrator).		Palo Alto's URL Filtering is a subscription module of our Next Generation Firewall platform. Therefore, this cannot be turned on as default, or enforced out of the box. However, if this subscription is purchased with the solution, we can enforce the filtering with the URL subscription in place. All of the URL filters must be locally configured on the appliance by a super administrator, and once configured, any end-users, such as students or teachers/members of staff, including administrators, will not be able to bypass them.

Describing how their system manages the following illegal content

Content	Explanatory notes – Content that:	Rating	Explanation
child sexual abuse	Content that depicts or promotes sexual abuse or exploitation of children is strictly prohibited and subject to severe legal penalties.		Palo Alto Networks URL filter can block all Illegal content using our categories of 'Questionable', 'Grayware', 'nudity', 'Adult ', and 'Extremism'. This enables schools to block websites that could provide access to content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties. Safe Search enforcement can also be implemented with multi-browser support to help block access to any websites that could contain this content.

			Data Filtering Profiles can also be used to create keyword alerts and report on sensitive, confidential, and proprietary information from leaving your network or users proactively searching for this content. Predefined patterns, built-in settings, and customizable options make it easy for you to scan files that contain or stop users searching terms using a regular expression of custom keywords relating to this topic and create a customized automated alert to meet these requirements.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual often occur in domestic contexts.		The Palo Alto URL filtering solution can block access to Categories of websites that could be used to manipulate, intimidate, or control a vulnerable person. These categories may contain legitimate websites such as 'blogs, Personal Sites and Blogs', 'Social networking', and 'questionable'. Palo Alto can also create a custom keyword search filter that can be implemented to create a custom list of search terms that can help protect users from accessing websites that could provide access to or become involved in psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts. Data Filtering Profiles can also be used to create keyword alerts and report on sensitive, confidential, and proprietary information from leaving your network or users proactively searching for this content. Predefined patterns, built-in settings, and customizable options make it easy for you to scan files that contain or stop users searching terms using a regular expression of custom keywords relating to this topic and create a customized automated alert to meet these requirements. Safe Search enforcement can also be implemented with multi-browser support to help block access to any websites that could contain this content.
extreme sexual violence	Content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, is illegal under UK law.		Palo Alto Networks blocks all Illegal content using our URL Filtering under the categories of 'Questionable', 'Grayware', 'nudity', 'Adult,' and 'Extremism' related categories. This enables schools to block websites that could provide access to extreme sexual violence content and is defined as illegal under UK law.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury is		Palo Alto Networks blocks all Illegal content using our URL Filtering under the categories of 'Questionable', 'Grayware', 'nudity', 'Adult', and 'Extremism' related categories. This enables schools to block websites that

	deemed obscene and unlawful.		could provide access to extreme sexual violence content, which is defined as illegal under UK law. Palo Alto can also create a custom keyword search filter that can be implemented to create a custom list of search terms that can help protect users from accessing websites that could provide access to extreme pornographic materials. Safe Search enforcement can also be implemented with multi-browser support to help block access to any websites that could contain this content.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.		The Palo Alto URL filtering solution can help protect users from Fraud. We can do this by blocking categories such as ' Malware', 'Phishing', 'hacking', and 'grayware'. These categories will block users from accessing content that intends to secure unfair or unlawful financial gain, including phishing and scam activities. Palo Alto's Credential Phishing Prevention can also help prevent users from being exposed to Phishing sites disguised as legitimate websites with the intent to steal user information, especially the credentials that provide access to your network. Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials.
Racially or religiously aggravated public order offences	Content that incites hatred or violence against individuals based on race or religion, undermining public safety and cohesion.		Palo Alto's URL filtering solution can filter out content using these 2 categories **Questionable:** Websites containing tasteless humour, offensive content targeting specific demographics of individuals or groups of people. **Extremism:** Websites promoting terrorism, racism, fascism, or other extremist views discriminating against people or groups of different ethnic backgrounds, religions, or other beliefs. This category was introduced to enable adherence to child protection laws required in the education industry. In some regions, laws and regulations may prohibit access to extremist sites, and allowing access may pose a liability risk. Palo Alto can also create a custom keyword search filter that can be implemented to create a custom list of search terms that can help protect users from accessing websites that could provide access to content that exposes the user to racially or religiously motivated hatred or violence.

			Data Filtering Profiles can also be used to create keyword alerts and report on sensitive, confidential, and proprietary information from leaving your network or users proactively searching for this content. Predefined patterns, built-in settings, and customizable options make it easy for you to scan files that contain or stop users searching terms using a regular expression of custom keywords relating to this topic and create a customized automated alert to meet these requirements.
Inciting violence	Online material that encourages or glorifies acts of violence poses significant risks to public safety and order.		Palo Alto's URL filtering solution can filter out content using these 2 categories **Questionable:** Websites containing tasteless humour, offensive content targeting specific demographics of individuals or groups of people. **Extremism:** Websites promoting terrorism, racism, fascism, or other extremist views that discriminate against people or groups of different ethnic backgrounds, religions, or other beliefs. This category was introduced to enable adherence to the child protection laws required. In the education industry. In some regions, laws and regulations may prohibit access to extremist sites, and allowing access may pose a liability risk. Palo Alto can also create a custom keyword search filter that can be implemented to create a custom list of search terms that can help protect users from accessing websites that could expose a user to Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.
Illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.		Palo Alto's URL filtering solution can filter out content using these 2 categories **Questionable;** Websites containing tasteless humour, offensive content targeting specific demographics of individuals or groups of people. **Extremism,** Websites promoting terrorism, racism, fascism, or other extremist views that discriminate against people or groups of different ethnic backgrounds, religions, or other beliefs. This category was introduced to enable adherence to child protection laws required In the education industry. In some regions, laws and regulations may prohibit access to extremist sites, and allowing access may pose a liability risk.

			Grayware can help filter content that could provide access to attempt on end users to grant access to illegal activities, criminal activities, unsolicited applications that could provide access to illegal immigration and people smuggling.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide poses serious risks to vulnerable populations.		Palo Alto's URL filtering can block access to URL categories that contain that can promote and Facilitate Suicide by blocking the category 'Abused Drugs', As well as implementing and enforcing Safe Search for supported browsers. Palo Alto could even block access to legitimate URLs that are under the categories of 'Personal Sites and Blogs', 'Social networking', and 'questionable', to provide even greater controls around this content. Palo Alto can also create custom keyword search filters that can be implemented to block access to a list of search terms related to self-harm and suicide, that can block access to web content that could expose a user to Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.to Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order. Data Filtering Profiles can also be used to create keyword alerts and report on sensitive, confidential, and proprietary information from leaving your network or users proactively searching for this content. Predefined patterns, built-in settings, and customizable options make it easy for you to scan files that contain or stop users searching terms using a regular expression of custom keywords relating to this topic and create a customized automated alert to meet these requirements.
Intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.		Palo Alto's URL filtering solution can provide the ability to block access to websites that host adult and inappropriate content that may contain these images by filtering the URL categories 'Nudity', 'adult', 'grayware', and 'Extremism'. This will filter out web content that is hosting and sharing non-consensual sexual images or videos otherwise described as "revenge porn".
selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms contravening legal regulations.		Palo Alto's URL filtering solution can provide the ability to block access to websites that advertise or promote the sale of prohibited substances or firearms, contravening legal regulations using the categories: 'Abused Drugs', 'grayware', ' weapons ', and 'Extremism'.

sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.		Palo Alto Networks blocks all Illegal content using our URL Filtering, by enabling the filter for 'Grayware' 'nudity', 'Adult', and 'Extremism' related categories. This enables schools to block websites that could provide access to extreme pornography.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.		Palo Alto Networks URL Filtering provides an 'Extremism' related category enabling schools and colleges to block websites that promote terrorism, racism, fascism, and other related extremist views that discriminate against people or groups from different ethnic backgrounds, religions, faiths, or beliefs.

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm and describe how their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Gambling	Enables gambling		Palo Alto Networks URL Filtering provides a 'Gambling' related category, enabling schools and colleges to block websites that promote and offer both legal and illegal gambling activities
Hate speech / Discrimination	Content that expresses hate or encourages violence towards a person or group based on something such as disability, race, religion, sex, or sexual orientation. Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010		Palo Alto can also create a custom keyword search filter using the Custom URL category that can be implemented to block access to a list of search terms related to content that expresses hate, or encourages violence towards a person or group based on something such as disability, race, religion, sex, or sexual orientation.
Harmful content	Content that is bullying, abusive, or hateful. Content that depicts or encourages serious violence or injury. Content that encourages dangerous stunts and challenges, including the ingestion, inhalation, or exposure to harmful substances.		Palo Alto's Advanced URL filtering solution can provide the ability to block access to websites that advertise or promote the sale of prohibited substances or firearms, contravening legal regulations using the categories: 'Abused Drugs', 'grayware,' 'weapons', and 'Extremism'. Palo Alto can also create a custom keyword search filter using the Custom URL category that can be implemented to block access to a list of search terms related to content that expresses hate or encourages violence

			towards a person or group based on something such as disability, race, religion, sex, or sexual orientation.
Malware / Hacking	promotes the compromising of systems, including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Palo Alto Networks Advanced URL filtering provides an option to block URLs categorised as 'High Risk' Sites whose domain was identified by the ML model to have properties previously linked to known malicious domains or had low web reputation signals. and sites hosting malware, phishing, or command-and-control (C2) sites The URL filter can also be configured to block. 'Malware', 'phishing', 'Hacking', and 'Ransomware,' which enable the blocking of sites that relate to illegal or questionable access to or the use of communications equipment/ software. The development and distribution of programs, how-to advice, or tips that may result in the compromise of a network. This also includes sites that facilitate the bypass of licensing and digital rights systems and protections, or sites containing and distributing malicious content, executables, scripts, viruses, trojans, and other malicious code. This solution can also provide further protection against 'command and control' if this category is enabled for URLs and domains used by hackers and Malware to take control of compromised or vulnerable systems. Surreptitiously communicating with the attackers' remote servers to send and receive malicious commands or exfiltrate the organisation's data. Palo Alto Firewalls and filtering systems have been ranked as a leader in the industry in third-party tests and cyber security benchmarking bodies, such as Gartner@ and Forrester@ ,for over 12 years consecutively.
Mis / Disinformation	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content		Palo Alto Networks Advanced URL Filtering provides a 'Questionable' category which enables the blocking of sites that contain tasteless humour, offensive content and

	undermining trust in factual information or institutions		targeting specific demographics of individuals or groups of people, criminal activity, illegal activity, violence, suicide, and pyramid / get-rich-quick schemes, and potentially mis/ Dis information. This can be paired with a custom search term filter to include key search words/ terms around the topics of concern, such as vaccines, conspiracy theories, and myths to enhance the filtering of search results to reduce the access or exposure to mis/ dis information and proactively encourage the user towards factual information.
Piracy and copyright theft	Includes illegal provision of copyrighted material		Palo Alto Networks Advanced URL filtering provides a 'copyright infringement' category, which enables the blocking of web pages and services that are dedicated to illegally offering access to videos, movies, and other media and software for download, which infringes copyright law. This can stop Peer-to-Peer and file exchange services, or general streaming services which provide access to films and other media. We can also enable the 'peer-to-peer' category specifically for sites that provide access for clients on the network to share and download content too.
Pornography	displays sexual acts or explicit images		Palo Alto Networks Advanced URL Filtering provides an 'adult' Category, which enables the blocking of sites containing sexually explicit materials, media (including language), art, and/ or products, online groups or forums that are sexually explicit in nature. Sites that promote adult services such as video/ telephone conferencing, escort services, strip clubs, etc. Anything containing adult content (even if it's games or comics) will be categorised as adult. We also provide a further ' nudity' category, which enables the blocking of sites that contain nude or semi-nude depictions of the human body, regardless of context or intent, such as artwork that includes nudist or naturist sites containing this kind of content and images.

Self-Harm and eating disorders	content that encourages, promotes, or provides instructions for self-harm, eating disorders, or suicide		Palo Alto Networks Advanced URL Filtering provides a 'Questionable' category, which enables the blocking of sites that contain tasteless humour, offensive content, and targeting specific demographics of individuals or groups of people, criminal activity, illegal activity, violence, suicide, and pyramid / get-rich-quick schemes. This can help to filter out content that encourages, promotes and/or provides instructions for self-harm, eating disorders, or suicide. Alongside this Palo Alto can also create a custom Filtering category for keyword search terms to filter content that could encourage, promote, or provide a student access to instructions for self-harm, eating disorders, or suicide too.
Violence Against Women and Girls (VAWG)	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.		Palo Alto Networks Advanced URL Filtering provides a 'Questionable' category, which enables the blocking of sites that contain tasteless humour, offensive content, and targeting specific demographics of individuals or groups of people, criminal activity, illegal activity, violence, suicide, and pyramid / get-rich-quick schemes. Palo Alto can also create a custom Filtering category for keyword search terms to filter content could provide access to a list of terms related to content that expresses hate or encourages violence, abuse of any kind including targeting women and girls, coercion or expressing hate towards harmful stereotypes or perpetuates misogyny.

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Our AI-powered detection can automate and enable rapid, highly accurate web filtering to eliminate threats live. This can also be used to help improve the category filtering by applying the same techniques to improve the detection of newly registered, or unknown URLs live. The URL filter can review image content, language to determine benign or malicious content. We use text and language analysis to draw correlations between website copy, the context in which the copy is used, and URLs to precisely categorise websites. Images from websites are broken down and compared to previous examples using sophisticated algorithms to assist in the determination of

possible malicious content links and phishing attacks. By examining each component of an individual page and applying multiple machine learning classifiers, we combine accuracy, speed, and continual adaptation in the face of changing attack techniques.
Content analysis; Palo Alto's NGFWs URL filtering uses crawlers to scrutinise multiple websites' attributes for malicious indicators and to help categorize the websites. Correlated domain data, the presence of forms, and the location of specific types of content are among the attributes our learning classifiers process. Every URL we analyse adds to our data library, continually informing and improving our ability to provide an up-to-date library of websites that may pose a security or safeguarding risk.
Text Analysis; Palo Alto Networks URL filtering scans websites, text, and their context to determine the most accurate category classifications. Keyword search filtering can block users from accessing and seeing inappropriate content by predefined terms relating to self-harm, hate speech, and adult and inappropriate or foul language.
Image Analysis: To avoid detection, phishing pages increasingly use obfuscated JavaScript and images on web pages instead of actual text. By automatically analysing the image content of each URL we can compare website code with visual indicators to more accurately determine whether a URL poses a phishing threat. We can also block inappropriate images by enforcing safe search.
Tight controls over common Policy Evasion Techniques; Palo Alto can enforce tight controls and common policies using user-ID and user-based DNS, application control, and URL filtering policies. These technologies could be used to mask or hide user activity on the network and bypass more traditional static URL/ DNS filtering tools.
Search Engine-Cached Result prevention: The Palo Alto URL filtering policies can be enforced even when users use common evasion tactics, such as cached results and language translation sites.
Translation Site Filtering: Palo Alto Networks URL filtering can block access to these sites that are often used to evade traditional URL and DNS based filtering tools.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to which the identification of individuals is retained and the duration for which all data is retained.

Retention and logging: Retention times for data logging on the firewall are established by your system administrator. Requests for categorisation, or uncashed URLs sent to PAN-DB URL filtering are entertained for six months, but this can be extended using Strata Cloud Manager for extended logging and reporting, and integrations with third-party reporting and monitoring tools can extend this beyond 12 months.

Providers should be clear about how their system does not overblock access, so it does not lead to unreasonable restrictions

Customizable Categories; Although the URL filtering can apply predefined categories, different organisations may wish to customise this around age, risk and tolerance and compliance, and area

of study. To meet this requirement, administrators can apply custom categories by combining multiple existing categories to create new ones or apply different rules based on the User ID or group.
Customizable Administrator / End-user Notifications: Administrators can create custom reports and schedule these to be sent to non-technical members of the team. We can also create email alerts based on rules and policy breaches.
URL Filtering Continued; When a user accesses pages that may pose a risk to the organisation or the user themselves, the URL filtering can present them with a custom warning page with a continue option if required. This presents the user with an opportunity to educate themselves or at least be aware of the risk before proceeding.
URL Filtering Override; Palo Alto's NGFW can also provide an override option for specific predefined categories that may be required for specific areas of study that need authorisation to access. This can be provided to senior members of the SLT to apply at the appropriate times.
Warning pages: When a user accesses pages that may pose a risk to the organisation or themselves, the URL filtering can present them with a custom warning page with a continue option if required or just a block page. This presents the user with an opportunity to educate themselves or at least be aware of the risk before proceeding.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Context-appropriate differentiated filtering, based on age, vulnerability, and risk of harm – also includes the ability to vary filtering strength appropriate for staff		Using the Pan-OS User ID, schools and colleges can create user and group-based security policies. This means that the IT team can allow, deny, and monitor all of the user's online activity, including URL categories or specific websites and applications, to stop users from misusing the system and only access age-appropriate content.
• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services, DNS over HTTPS, and ECH.		Palo Alto Networks NGFW provides tight controls over common policy evasion techniques employed by users. The URL filtering policies can be enforced even when users use common evasion tactics, such as cached results and language translation sites. Blocking Search Engine Cached Results: Palo Alto can block a common tactic used to evade controls, accessing cached results within popular search engines. Embedded activity within applications: Some applications can mask activity and hinder the ability to enforce safe search. Palo Alto has the ability to enforce users to only access approved

		applications to help with Safe Search enforcement. Translation sites, Palo Alto Networks URL filtering can block access to these sites that are often used to evade URL filtering. Pal Altos Application control and DNS security features can help to contain users to only approved and monitored applications as well as DNS protocols being abused by rogue applications to circumvent the web filtering system.
• Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged, enabling an audit trail that ensures transparency and that individuals are not able to make unilateral changes		The Palo Alto Networks NGFW solution is fully customisable, and the administrator remains in full control of all reports and filtering on the system at all times. Any required changes, audits, or reports can be applied or run instantly at any time. Providing full granular control of the system.
• Contextual Content Filters – in addition to URL or IP-based filtering, Schools should understand the extent to which (http and https) content is dynamically analysed as it is streamed to the user and blocked. This would include AI or user-generated content, for example, being able to contextually analyse text and dynamically filter the content produced (for example, ChatGPT). For schools' strategy or policy that allows the use of AI or user-generated content, understanding the technical limitations of the system, such as whether it supports real-time filtering, is important.		Palo Alto has the ability to apply keyword filters by creating a Custom URL category with search queries for specific predefined words. We can do this by creating a Log Forwarding Profile with a filter for the URL categories to be alerted. Data Filtering Profiles can also be used to create keyword alerts and report on sensitive, confidential, and proprietary information from leaving your network or users proactively searching for this content. Predefined patterns, built-in settings, and customizable options make it easy for you to scan files that contain or stop users searching terms using a regular expression of custom keywords relating to this topic and create a customized automated alert to meet your KCSIE safeguarding needs. Palo Alto has also introduced the AI Filtering category into our URL filtering solution. By default, we set the "Artificial Intelligence" category to "Alert" mode for the default profile only. If you have multiple URL Filtering profiles, we recommend that you change the default action from "Alert" to "Block" for this category in each of your profiles.
• Deployment – filtering systems can be deployed in a variety (and combination) of ways (e.g., on device, network level, cloud, DNS). Providers		Palo Alto Networks is one of the few vendors on the market that has consistent feature parity across our platform of solutions, regardless of deployment method. We offer and support the

should describe how their systems are deployed alongside any required configurations		deployment either on premise or in the cloud and can offer a physical, virtual (VM), or SASE (Cloud delivered) filtering solution that can be deployed to meet your needs in any environment. The URL filtering can also be deployed as a web proxy if required to work alongside a third-party solution or in conjunction with another vendor.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering, with classification and categorisation as well as how the system addresses overblocking		Palo Alto Networks filtering can be fully customised to meet your safeguarding and prevent needs. A full list of our category filters can be found on our website.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight, or a dashboard		Palo Alto has the ability to provide Group or multi-site management with central policies via our Panorama management and reporting platform that can centrally control multiple firewalls.
● Identification - the filtering system should have the ability to identify users and devices to attribute access (particularly for mobile devices) and allow the application of appropriate configurations and restrictions for individual users. This would ensure safer and more personalised filtering experiences.		Palo Alto Networks provides the ability to identify individual users, what content, and what applications they are accessing at any time on any device by syncing with the active directory and your wireless/authentication system.
● Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from those delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser-delivered content). Providers should be clear about the capability of their filtering system to manage content on mobile and web apps, and any configuration or component requirements to achieve this		Palo Alto Networks URL Filtering and Application Control can help restrict users to only approved and monitored applications. This includes Mobile and device applications for both managed and unmanaged devices.
● Multiple language support – the ability for the system to manage relevant languages		Palo Alto Networks supports over 41 different languages, which can be found on our website.
● Remote devices – with many children and staff working remotely, the ability for school-owned devices to receive the same or equivalent filtering as that provided in school		Palo Alto can secure all managed devices remotely using a GlobalProtect client installed on the device. This can enforce the same level of filtering on the device, anytime, anywhere. This solution can be enforced to be always on and supports

		Windows and Mac in the base licence and Android, IOS, and a limited set of Chrome and Linux devices in the premium licence. You can learn more about this in our Supporting Remote Learning white paper
• Reporting mechanism – the ability to report inappropriate content for access or blocking		All Palo Alto hardware and Virtual Firewall come with on-box reporting and monitoring included. User-ID can be configured to monitor and filter authenticated events at a network level. This allows User-ID to associate a user with the IP address of the device from which they are logged in and does not therefore rely on any other form of software.
• Reports – the system offers clear, granular historical information on the websites users have accessed or attempted to access		All of the created reports can be scheduled to be sent to all appropriate members of the team, both technical and non-technical, at set intervals or times during the day. We can also create alerts if specific categories or filters are hit.
• Safe Search – the ability to enforce 'safe search' when using search engines		Safe Search can be enforced on all users' devices, regardless of whether they are managed or unmanaged. This can be enabled in the URL filtering policy for all users and will enforce safe search on all approved browser applications, such as Edge and Chrome, ensuring that students and staff have approved access to the internet. The safe search results are updated and maintained by Google and not Palo Alto.
• Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand the context of activity		Palo Alto does not currently integrate with Safeguarding case management systems, however, we do have Api's and integrations with third-party monitoring and reporting tools that do.

How does your filtering system manage access to Generative AI technologies (e.g., ChatGPT, image generators, writing assistants)?

In your response, please describe whether and how your system identifies, categorises, or blocks Generative AI tools; how access can be controlled based on age, risk, or educational need; any limitations in filtering AI-generated content—particularly where such content is embedded within other platforms or applications; and what support or configuration guidance you offer to schools to help them align with the UK Safer Internet Centre's Appropriate Filtering Definitions and relevant national safeguarding frameworks.

Palo Alto Networks' AI Access Security enables organizations to embrace GenAI applications responsibly. Schools can confidently adopt AI without sacrificing end-user security and confidence in protecting the institution's data through visibility into AI applications, fine-grained access controls, and a robust data protection framework.

Palo Alto has also introduced the AI Filtering category into our URL filtering solution.

By default, we set the “Artificial Intelligence” category to “Alert” mode for the default profile only. If you have multiple URL Filtering profiles, we recommend that you change the default action from “Alert” to “Block” for this category in each of your profiles.

The "Artificial Intelligence" category can be utilized to formulate a policy framework around the generative AI websites that your users can visit and interact with, or the services that are in use in your development environments. Category allows you to take flexible actions based on your company's requirements and needs.

For instance, the category can be leveraged for:

- SSL decryption to gain complete visibility and a comprehensive view of AI services and usage.
- Striking a balance with intelligent access controls that allow you to either: Block access when necessary, or extend caution-based access with a “Continue” page that coaches users about the potential risks associated with generative websites and tools.

Additional Information
For more information on best practices when managing Advanced URL Filtering categories, please read our:-
URL Filtering Category Recommendations
Complete List of PAN-DB URL Filtering Categories

Filtering systems are only ever a tool in helping to safeguard children when online, and schools have an obligation to “*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*”.[1]

Please note below the opportunities to support schools (and other settings) in this regard

Palo Alto Networks Cyber Academy offers Faculty Training, hands-on Labs, Modularized curriculum, and virtual firewall training at no cost to qualified academic institutions. A list of institutions that we already work with in the UK can be found here:- https://www.paloaltonetworks.co.uk/services/education/authorized-academy-centers/authorized-academy-centers#emea

Palo Alto also offers FREE End-user training from our Beacon platform to enable end-users to maximise the return on their investment and get the most out of their security tools or prepare for accredited exams. This is Palo Alto Networks' free digital courses so that you can learn at your own pace. These courses cover all elements of our technology, from product fundamentals to specialised role-based learning.:- https://beacon.paloaltonetworks.com/student/catalog

We also have an education program for Lower education, Cyber A.C.E.S. includes Activities in Cybersecurity Education resources to help demystify cybersecurity through interactive learning, designed for children ages 5 to 15 with an understanding of how to protect their digital future. https://start.paloaltonetworks.com/cyber-aces.html

Cyber A.C.E.S. provides the cybersecurity basics students need to have safer online experiences and become good digital citizens. Lessons are designed so they can be facilitated by anyone, regardless of their knowledge level, with each module tailored to a specific age group.

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Provider Self-Certification Declaration

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Initial
RC

Name	Natascha Nikolic
Position	Senior Manager, Commercial Finance EMEAL
Date	2025-09-24
Signature	Signed by: Natascha Nikolic C4E22C0867264F0...