Appropriate Filtering for Education settings

UK Safer Internet Centre
www.saferinternet.org.uk
brought to you by SWGfL Childnet IWF

May 2025

Filtering Provider Checklist Reponses

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) meets the national 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	Sophos Ltd
Address	The Pentagon, Abingdon Science Park, Barton Lane, Abingdon, Oxfordshire, OX143YP
Contact details	Roger.Neal@sophos.com
Filtering System	Sophos Firewall OS (SFOS) is installed on the Sophos XGS Firewall Solutions. This Firewall solution is available as physical, public cloud based or virtual Appliances to provide convenience to customers. The platform is designed to be Secure By Design, to comply with DfE cyber security standards and NCSC Cyber Security recommendations like Cyber Essentials. The firewall platform is designed as a modular solution which can be used as a dedicated web filtering proxy solution or as part of a XStream Firewall solution – this is depending on licensing purchased by the customer.
Date of assessment	18th August 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.	

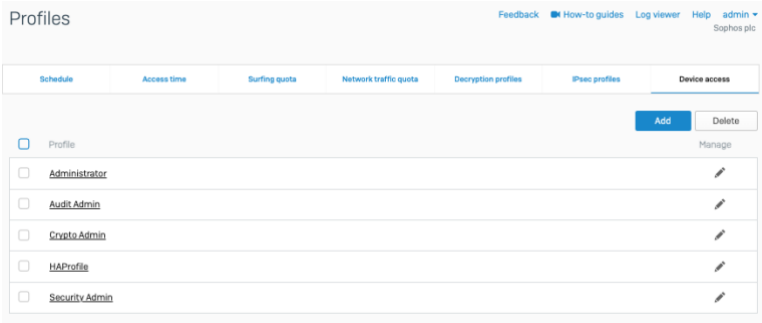
.

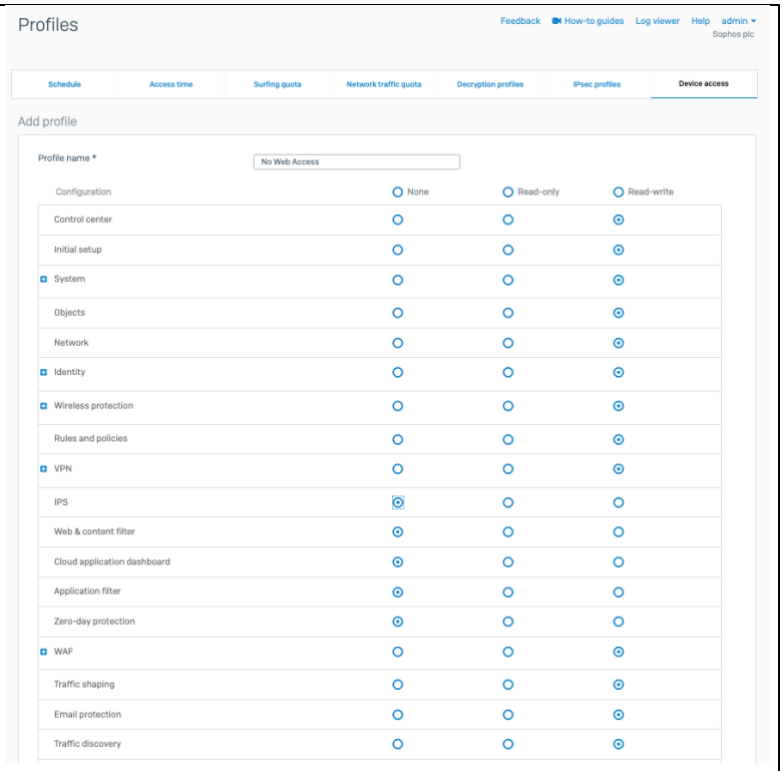
Illegal Online Content

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

Aspect	Rating	Explanation
• Are IWF members	Green	Yes, Sophos is a member of the Internet Watch Foundation and routinely works with the IWF and other agencies in helping to identify the methods used by child abusers to share content, reporting the discovery of child abuse images online.
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list), including frequency of URL list update	Green	Yes, Sophos actively implement the IWF CAIC list. This list is updated every 6 hours as a maximum candace.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	Green	Yes, Sophos include the Counter Terrorist (CTIRU) lists published by authorities.

• Confirm that filters for illegal content cannot be disabled by anyone at the school (including any system administrator).	Amber	As noted, the Sophos Firewall is a modular Next Generation Firewall solution used by over 300,000 customers globally with flexible licensing options to suit customer specific requirements within one single solution. For educational setting use we recommend the Xstream Protection licence, which includes the Web Protection, Day Zero Protection (sandboxing of file downloads), Base Firewall, Network protection, Management in Sophos Central and Technical Support. See https://docs.sophos.com/central/customer/help/en-

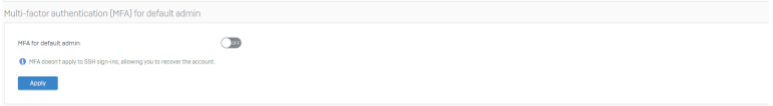
		us/LicensingGuide/FirewallLicenses/SFOSLicensingModel/index.html for more details on licensing options. Because of this license flexibility, the solution includes granular Role Based Administration and Auditing to allow system users to define specific roles and responsibilities to IT teams as per good IT Practice (and UK Department for Education Cyber Security Standards). Typically, in education, the IT Manager is setup as the "Super Admin", who has overall management responsibilities of the entire platform and associated cyber risks registered on the school's risk register. The IT Manager will delegate specific roles and responsibilities to other team members, who manage day to day activities on the solution. Such as rule changes, policy updating, reporting, log monitoring as per the DfE's other cyber requirements and Safeguarding. This "Super Admin" will then either use existing pre-defined roles within the Sophos Firewall (see screenshot below) or create new roles and assign these specific role rights to the IT team and DSL's as required.  It is as simple as clicking Add to create a new role that has all rights to the web filtering component / policies / setup completely removed (note the None column below).



This role is then assigned by the Super Admin to other system admins, so they can perform their other day to day tasks on the system as required for their job role. But completely removing any ability to modify web setup on the platform.

If web filtering is enabled and configured on the Firewall solution. The IWF list or illegal content cannot be bypassed for web traffic by users or admins without the Super Admin role and web role rights.

The Sophos admin should also enable multi factor authentication to the admin portal to add an extra layer of protection for the default admin.



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, which is strictly prohibited and subject to severe legal penalties.	Green	Yes, Sophos is a member of the Internet Watch Foundation and routinely works with the IWF and other agencies in helping to identify the methods used by child abusers to share content, reporting the discovery of child abuse images online. These lists

			are marked as “High Risk” and blocked by default.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.	Green	Sophos provides an “Intolerance and Hate” category to enable blocking of sites that provide content relating to controlling or coercive behaviour and blocked by default.
extreme sexual violence	Content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, and is illegal under UK law.	Green	Sophos provides “Extreme” and “Criminal Activity” categories. Sophos recommends blocking these categories to restrict sites displaying or promoting the viewing of extreme sexual violence and blocked by default.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury and is deemed obscene and unlawful.	Green	Sophos provides an “Sexually Explicit” category to enable blocking of sites that Sites Adult sites not falling in "Porn, Nudity, Swimwear & Lingerie, Sex Education, and Sexual Health & Medicines" will be included in "Adult Content" and which may contain material not suitable to be viewed for audience under 18. and blocked by default.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.	Green	Sophos provides an “fraud” category to enable blocking of sites that Sites gathering personal information (such as name, address, credit card number, school, or personal schedules) that may be used for malicious intent and blocked by default.
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.	Green	Sophos provides an “Intolerance and Hate” category to enable blocking of sites that foster racial supremacy or vilify/discriminate against groups or individuals and blocked by default.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.	Green	Sophos provides “Extreme” and “Criminal Activity” categories. Sophos recommends blocking these categories to block sites displaying or promoting the use of physical force intended to hurt or kill. blocked by default.
illegal immigration	Content that promotes or facilitates unauthorized entry into a country, including services	Green	Sophos provides “Criminal Activity” categories. Advocating, instructing, or giving advice on

and people smuggling	offering illegal transportation or documentation.		performing illegal acts such as illegal immigration and people smuggling. Blocked by default.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.	Green	Sophos provides “Criminal Activity” categories. Advocating, instructing, or giving advice on performing illegal acts such as phone, service theft, evading law enforcement, lock-picking, burglary techniques and suicide. and blocked by default.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.	Green	Sophos provides an “Sexually Explicit” and “Criminal Activity” categories to enable blocking of sites that may contain material not suitable to be viewed and blocked by default.
selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.	Green	Sophos provides “Controlled Substances” and “Weapons” categories. Sites providing information about or promoting the use, trade or manufacture of drugs other than marijuana that are controlled or regulated in most jurisdictions and Sites providing information about, promote, or support the sale of weapons and related items. Sophos Recommend blocking these sites
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.	Green	Sophos provides “Criminal Activity” categories. Advocating, instructing, or giving advice on performing illegal acts such as sexual exploitation and blocked by default.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.	Green	Sophos provides “Criminal Activity” categories. Advocating, instructing, or giving advice on performing illegal acts such as those related to Terrorism and blocked by default.

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	Green	Sophos provides an “gambling” category to enable blocking of sites that foster or encourage gambling habits. Sophos recommends blocking this category.
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	Green	Sophos provides an “Intolerance and Hate” category to enable blocking of sites that foster racial supremacy or vilify/discriminate against groups or individuals. Sophos recommends blocking this category.
Harmful content	Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.	Green	Sophos provides an “Intolerance and Hate” category to enable blocking of sites that foster racial supremacy or vilify/discriminate against groups or individuals. Sophos recommends blocking this category.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	Green	Sophos prevents access to sites containing malware by default. The solution also provides a “Hacking” category to enable blocking of sites that contain or promote sites relating to malware and hacking. Sophos recommends blocking this category. Categories are also provided for “Anonymizers”, “Phishing and Fraud”, “Spam URLs” and “Spyware and Malware” categories. Sophos recommends blocking these categories. In addition, all unencrypted http and https (recommended this is scanned) content is scanned for malware. A cloud-delivered sandbox analyses any downloaded active content and blocks malware.
Mis / Dis Information	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content undermining trust in factual information or institutions	Green	Sophos provides an “Intolerance and Hate” category to enable blocking of sites that foster Mis / Dis Information. Sophos recommends blocking this category.

Piracy and copyright theft	includes illegal provision of copyrighted material	Green	Sophos provides “Peer to peer and torrents” and “intellectual piracy” categories. Sophos recommends blocking these categories.
Pornography	displays sexual acts or explicit images	Green	Sophos provides “Sexually Explicit”, “Nudity” and “Extreme” categories. Sophos recommends blocking these categories. Also, Sophos provides “Safe Search” enforcement on the major search engines. The option is also available to add a “Creative Commons” license that only shows images published under Creative Commons licensing laws. To date, using this method has not resulted in any pornographic images being forwarded to Sophos for reclassification.
Self Harm and eating disorders	content that encourages, promotes, or provides instructions for self harm, eating disorders or suicide	Green	Sophos provides the “Pro-suicide and self-harm” category. Sophos recommends blocking this category.
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.	Green	Sophos provides “Extreme” and “Criminal Activity” categories. Sophos recommends blocking these categories to block sites displaying or promoting the use of physical force intended to hurt or kill.

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

Sophos currently provides 91 different URL categories. For the full list see: https://www.sophos.com/threat-center/reassessment-request/utm.aspx.

Sophos Labs enables us to dynamically update our web categories by providing a URL categorisation services that integrate Sophos URL data with that of multiple third-party suppliers, including IWF and CTIRU, to provide a market-leading database.

Sophos classifies sites at the IP level, domain, sub-domain and path URL data is constantly reviewed and unclassified websites are classified on an hourly basis.

Customers can create their own URL lists for blocking / allowing and can request recheck or reclassification directly from sophos via the sophos web site https://support.sophos.com/support/s/filesubmission?language=en_US

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

Sophos Firewall retain reports on box for up to a year. This retention period can be potentially impacted by disk space which is checked during the scoping phase with Sophos engineers. As the disk reaches its maximum capacity it will delete the eldest records. Therefore, if the box has additional work to do that wasn't covered in the scoping it's possible that the retention phase is reduced.

We recommend customers choose to use Central Reporting Advanced which would give 30 days of reporting with an XGS Xstream license, with options to increased storage through the purchase of data blocks. Data Blocks are available for purchase to meet a schools retention needs or purchase additional data storage packs for longer storage on Sophos Central.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Sophos category database protects more than 600,000 organizations in more than 150 countries with over 300,000 Firewall customers using over 500,000 Sophos Firewalls solutions.

The huge amount of telemetry helps Sophos to fine tune our web filtering policies based on the typical activities of users in different settings. Sophos also provides tools that enable customers to create custom categories that over-ride current URL database classifications and end-users to request page reclassification, by the system administrator, directly from the block page. Education establishments can therefore tweak their web filtering policies to make sure they are enabling their staff and students to be the best and brightest they can be. Safe in the knowledge that they are also helping keep their users safe online while also meeting the Department for Education requirements for Cyber Security, Safeguarding and Prevent.

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	Green	Sophos can apply policy rules based on group information. If the school includes objects related to age then policies can be created that open certain categories of websites once a certain age has been reached (e.g. the "Sex Education" category. Sophos also logs all user group activity separately for reporting. Reports can be generated for a specific event in a specific user group on box. Additionally all alerts can be sent using syslog into a Security Incident and Event Management system (SIEM) or 3rd party reporting tool such as Fastvue Reporter.
• 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.	Green	Sophos provides the "Anonymizers' category in our web filter. Sophos recommends blocking this category. Whilst we also provide a 'block filter avoidance app' application rule. Both policies would block users from being able to circumvent their filtering. Additionally, customers using the Firewall Functionality can use this module to block ports and protocols commonly used to circumvent web filtering solutions, such as outbound RDP, VPN, QUIC, DNS, ECH etc..
• 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 ensure transparency and that individuals are not able to make unilateral changes	Green	The day-to-day administration of the Sophos Firewall appliance is done by the school IT team (or partner if this is out-sourced), using the granular role based admin and auditing within the solution. There is complete flexibility in the policy model to create policies that can block categories, file types, URLs, IPs and much more. Policies can be created easily and intuitively using a very user-friendly interface.
• 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	Green	The Sophos Firewall includes a content scanning feature, whereby URLs and web pages are dynamically analysed for specific keywords or phrases. Customers can upload multiple keyword lists to support different languages and provide better granularity. Any pages matching words or phrases contained within the keyword lists can be blocked and/or logged. In addition,

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.		Administrators/Safeguarding officers can review the blocked keywords using the onboard log viewer and determine the context.
• Deployment – filtering systems can be deployed in a variety (and combination) of ways (eg on device, network level, cloud, DNS). Providers should describe how their systems are deployed alongside any required configurations	Green	The Sophos Firewall solution is available as a physical appliance, virtual appliance or as an image on AWS (bring your own licence or pay as you go) or on Azure. Network traffic is then passed through the appliance as required for Firewall or web filtering. Sophos recommends professional services or partner technical assistance in setting up to provide best practice and training on the solution to ensure compliance to DfE requirements for Cyber Security and Safeguarding requirements.
• 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 over blocking	Green	Sophos provides the rationale behind its web classification so that accurate choices can be made by IT administrators. This information can be found here: https://support.sophos.com/support/s/article/KB-000036518?language=en_US
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	Green	Sophos provides a central management console called Sophos Central. This platform enables you to manage multiple site based (MAT for example) and / or multiple Firewalls in one console. Central policy can be configured and pushed out to your different sites. Whilst reporting and alerting can all be managed centrally
• Identification - the filtering system should have the ability to identify users and devices	Green	Sophos Firewall can identify users transparently via Single-Sign on or through integration with directory server login processes or via the Sophos Endpoint Protection Client.

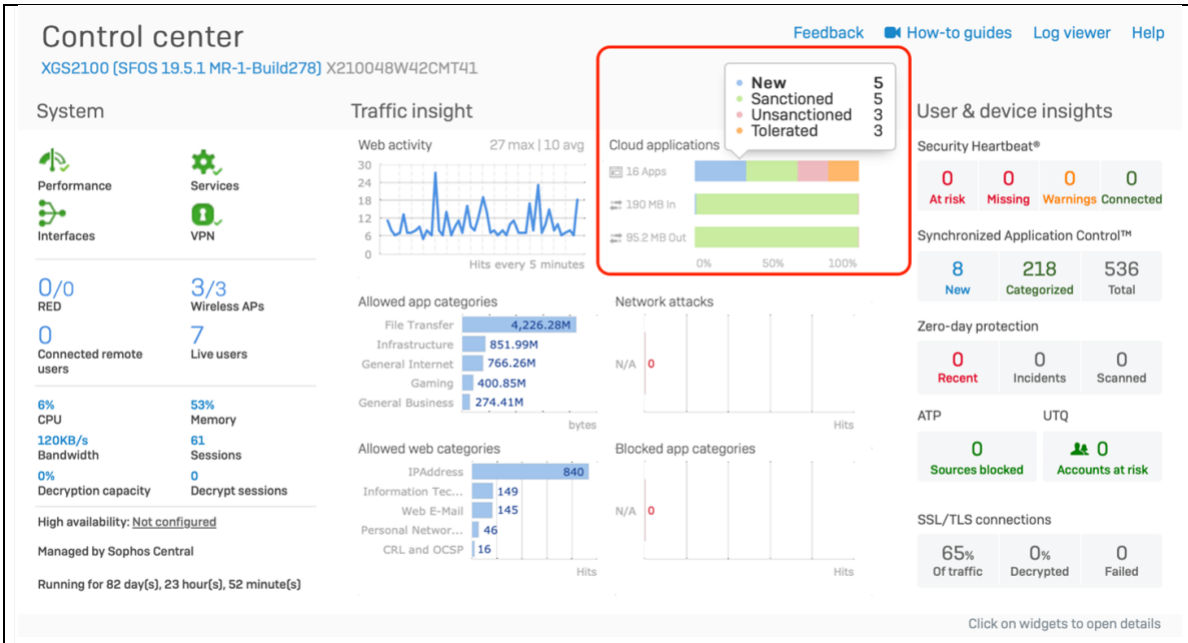
to attribute access (particularly for mobile devices) and allow the application of appropriate configurations and restrictions for individual users. This would ensure safer and more personalised filtering experiences.		It can also provide non-transparent authentication where a user is required to login before browsing.
• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that 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	Green	Sophos Firewall is able to filter all http and https connections including TLS 1.3 encrypted traffic. This is not limited to browser traffic and includes mobile and app connections. Sophos also provides policy-driven application control that can also identify and manage traffic that uses other protocols
• Multiple language support – the ability for the system to manage relevant languages	Green	Sophos Firewall supports multiple block pages to support multiple languages and custom block pages where multiple languages are required on the same page.
• Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school	Green	For Windows and Mac devices that are not on the school network, web filtering can be enforced using our Sophos Central Endpoint protection client (Intercept X Advanced). This includes web control, which has specific policies for remote devices. These policies can be managed via Sophos Central (our Cloud management platform) and any violations can be reported on. There are over 48 categories that can be configured, as well as file type blocking. This includes sites that are on the IWF and Counter Terrorism Referral Unit block lists.

		Webfiltering on Chromebooks can also be controlled via Sophos Mobile (UEM Solution).
• Reporting mechanism – the ability to report inappropriate content for access or blocking	Green	Sophos provides a number of built-in reports that can be used to see this information. These reports are fully customisable and can be emailed to admins/teachers/safeguarding officers. In addition, the log files can be exported using syslog to third party tools. Additionally through Syslog, 3rd party solutions like FastVue Reporter can also provide reporting.
• Reports – the system offers clear granular historical information on the websites users have accessed or attempted to access	Green	Sophos provides a number of built-in reports that can be used to see this information. In addition the log files can be exported using syslog to third party tools.
• Safe Search – the ability to enforce 'safe search' when using search engines	Green	Sophos supports Safesearch within web filtering policy
• Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity	Amber	The Sophos Solution currently supports email alerting, so if the safeguarding solution accepts email notifications fully supported.

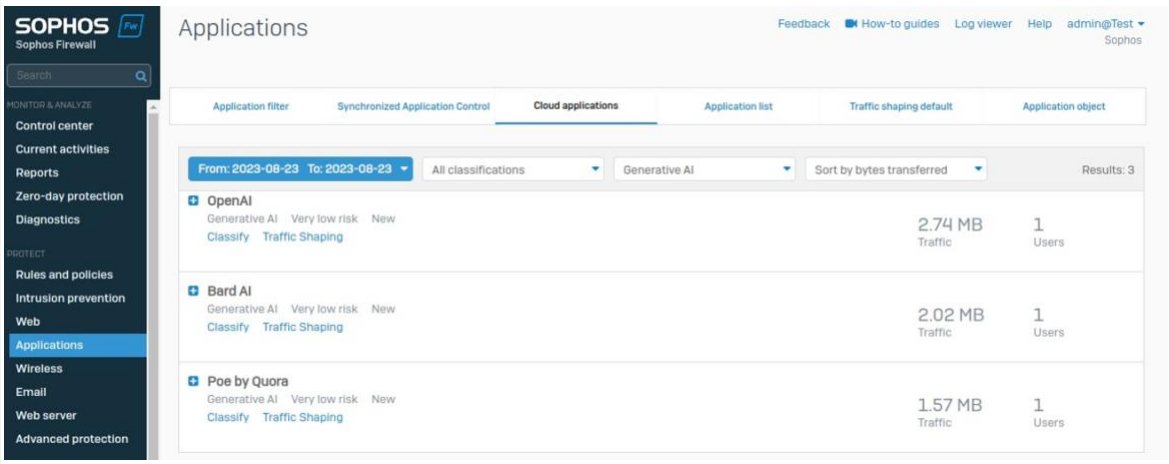
How does your filtering system manage access to Generative AI technologies (e.g. ChatGPT, image generators, writing assistants)?

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.

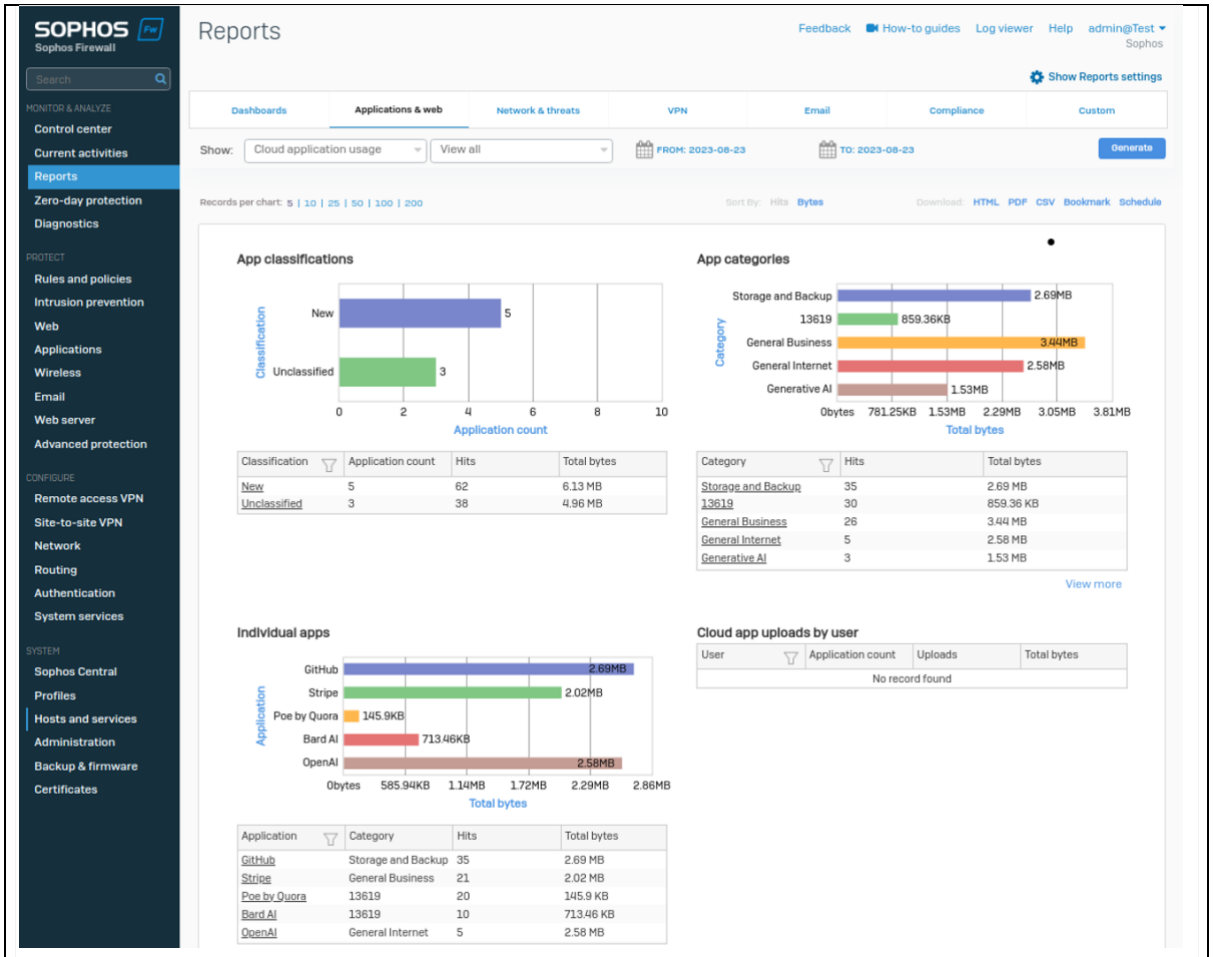
Sophos Firewall offers important features for easily monitoring and controlling cloud application usage with its in-line Cloud Access Security Broker (CASB) capabilities, which are highlighted on the Sophos Firewall Control Center. This offers a quick, at-a-glance solution to gain visibility into cloud applications – and now Generative AI usage – to identify and control shadow-IT usage and potential data loss vectors.



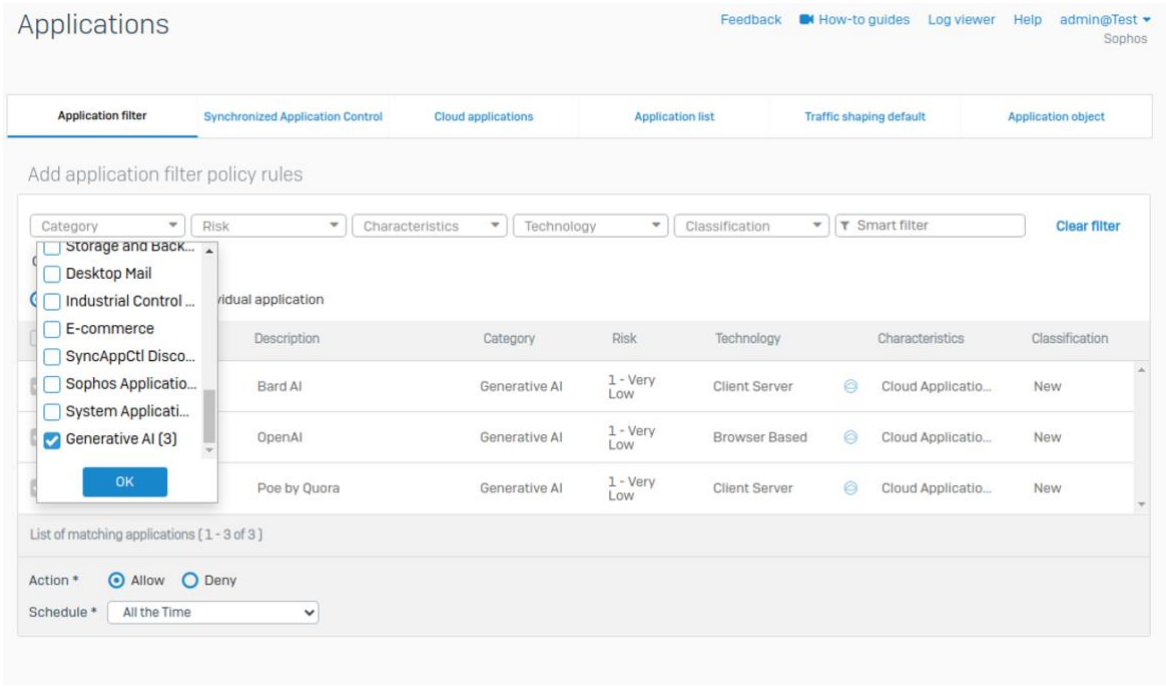
You can easily drill-down to see which specific cloud applications are being accessed on your network that are new, sanctioned, unsanctioned, or tolerated, and build policies to either accelerate, block, or shape this traffic. Generative AI application usage is listed alongside other cloud applications with full traffic volume and user details, providing quick insights and easy classification options:



Insights are also available in both the on-box and Sophos Central reporting as well as the firewall log viewer:



You can use the new Generative AI application signatures to easily add application control rules to enforce your desired policies:



Your firewall device will require either our Web Protection subscription or Xstream Protection bundle (which includes Web Protection) to utilize the application control and CASB cloud application capabilities.

You can check that you have received the new Generative AI signature update by navigating to "Backup & firmware > Pattern updates" and checking that the current version of IPS and Application signatures is version 18.20.86 or later.

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 opportunities to support schools (and other settings) in this regard

Sophos has introduced Sophos Home Premium (https://home.sophos.com). This provides home users access to enterprise-grade security software to block malware and enforce parental category controls for web traffic. In terms of education, Sophos in partnership with SWGFL has produced thousands of educational booklets that redistributed to schools nationwide to advise on online safety. Sophos organises student days where we invite students into our headquarters in Abingdon to learn how Sophos deals with the latest online threats and what students can do to protect themselves more effectively. Many universities use Sophos products as part of their curriculum to learn about filtering and antimalware technologies.

[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.

Name	Roger Neal
Position	Director Mid-Market and Commercial Pre-Sales UKI
Date	18th August 2025
Signature	Roger Neal