Appropriate Filtering for Education settings

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	Fortinet, Inc. (which is the manufacturer (not the supplier) of Fortinet network security products and related services)
Address	909 Kifer Road, Sunnyvale, 94086 California, United States
Contact details	+44 20 3752 6880
Filtering System	FortiGuard Web Content Filtering
Date of assessment	June 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	🟩	Fortinet subscribe and are a member of the IWF
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list), including frequency of URL list update	🟩	Fortinet include the list supplied by the IWF in our category based webfiltering under the category of **child sexual abuse.** This list is dynamically and centrally updated by FortiGuard services. URL list is dynamically referenced by the FortiGate through FortiGuard threat intelligence services, and is updated centrally as and when required.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	Fortinet subscribes to the Counter Terrorist Informational Referral Unit - CTIRU for the lists of URL's and domains which have this content.

● Confirm that filters for illegal content cannot be disabled by anyone at the school (including any system administrator).	🟧	System admin can disable configured filters however this can be prevented by use of a number of options. Option 1, If the deployed FortiGate/FortiGates are managed by a third-party restricted configuration access can be put in place. See admin profiles https://docs.fortinet.com/document/fortigate/7.6.4/administration-guide/294491/administrator-profiles Option 2, The system admin access can be subject to a 2FA access arrangement whereby a second person holds the token access code. This can be used to prevent liberal access to admin level configuration. Note two tokens are provided as standard on the FortiGate. See user profiles. https://docs.fortinet.com/document/fortigate/7.6.4/administration-guide/014906/administrator-account-options Option 3, FortiManager can be employed to provide workflow management which can be used to enforce config change approvals. See FortiManager workflow. https://docs.fortinet.com/document/fortimanager/7.6.4/administration-guide/424502/workflow-mode The FortiGate will log any changes made and these can be reviewed at any time.

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.	🟩	The Fortinet solution provides the ability under web filtering to block access to URL/Domains that contain this type of content. This is covered by enabling the webfiltering **category child sexual** abuse in the FortiGate webfilter profile which is contributed to by the IWF
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.	🟩	**Explicit Violence** web filter category -This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Where a site is not rated the **Unrated** category can be set to block as a catch all.

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.	🟩	**Explicit Violence** web filter category -This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Where a site is not rated the **Unrated** category can be set to block as a catch all.

extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.	🟩	**Explicit Violence** web filter category -This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Where a site is not rated the **Unrated** webfilter category can be used as a catch all.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.	🟩	**Illegal or Unethical** webfilter category - 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. Also the category **Phishing** webfilter category- Counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users.
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.	🟩	**Discrimination** webfilter category - Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.

inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.	🟩	**Explicit Violence** webfilter category - This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. **Terrorism** web filter category - 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 organizations.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.	🟩	**Illegal or Unethical** web filter category - 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.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.	🟩	**Explicit Violence** webfilter category - This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Where a site is not rated the **Unrated** category can be set to block as a catch all.

intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.	🟩	**Nudity and Risque** web filter category - Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse. **Other Adult Materials** web filter category - 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** web filter category - Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite. Where a site is not rated the **Unrated** category can be set to block as a catch all.
selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.	🟩	**Drug Abuse** webfilter category - Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc. Also the webfilter category **Weapons** - Websites that feature the legal promotion or sale of weapons such as hand guns, knives, rifles, explosives, etc.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.	🟩	**Other Adult Material** web filter category - 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** web filter category - Mature content
		🟩	websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite. Where a site is not rated the **Unrated** category can be set to block as a catch all.

Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.	🟩	**Terrorism** Webfilter category - 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 organizations.

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	🟩	**Gambling** webfilter category Sites that cater to gambling activities such as betting, lotteries, casinos, including gaming information, instruction, and statistics.
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	🟩	**Discrimination** webfilter category - Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.
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.	🟩	**Explicit Violence** web filter category -This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Where a site is not rated the **Unrated** category can be set to block as a catch all.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	🟩	**Malicious Websites** webfilter category - Sites that host software that is covertly downloaded to a user's machine to collect information and monitor user activity, and sites

		🟩	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. Also **Hacking** webfilter category - Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites.
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	🟩	**Alternative Beliefs** web filter category - Websites that provide information about or promote spiritual beliefs not included in Global Religion, or other nonconventional or folkloric beliefs and practices, including but not limited to sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, satanic, or supernatural beings. Where a site is not rated the **Unrated** category can be set to block as a catch all.
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	**Illegal or Unethical** web filter category - 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.
Pornography	displays sexual acts or explicit images	🟩	**Pornography** webfilter category - Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite.

General categorisation is based on an automated categorisation engine which has been developed in-house and which has evolved over more than 15 years since its initial conception. The system uses language dictionaries to allow support in any language. Sites are scanned based on a number of methods:

- new pages on identified popular sites
- URLs which are requested by a user, but which are not rated. Such URLs will go into a queue to be rated based on hit count and the current charge on the system.
- Bulk requests from a specific customer. Such requests are treated case by case, but we generally offer this as a free service.
- Individual requests received from customers or users. These requests can be received in a number of ways (see below) and may be either requests to rate an unrated site, or requests to change the rating of a site.

In general, initial rating is done by the automated rating system. Malicious content (viruses, exploits) is not rated using this system (more details below) because such sites generally have legitimate visible content.

Ratings may also be obtained from third-party feeds, including feeds from governments or other organisations, containing such content as extremism or sexual violence.

Requests to change the rating of an already categorised URL will always be dealt with by a human, to ensure that the request gets the highest level of care and attention

Self Harm and eating disorders	content that encourages, promotes, or provides instructions for self harm, eating disorders or suicide	🟩	**Explicit Violence** web filter category -This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Where a site is not rated the **Unrated** category can be set to block as a catch all.
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.	🟩	**Explicit Violence** web filter category -This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Where a site is not rated the **Unrated** category can be set to block as a catch all.

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

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.

Retention policy on the centralized logging platform is flexible and can be tuned and adjusted to suit the retention policy requirement. Additional to this it is possible to automate backups to secure storage, for archiving of logs, which can also be restored to the logging platform for reporting if required.

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

This is covered below, but to summarise:
A flexible hierarchical search system is used which allows ratings to be given to anything from a top-level domain or an IP address, right down to a fully-specified URL. This allows for example a blogging site such as wordpress.com to have a "Personal Websites and Blogs" rating, whilst individual blogs can have a rating based on their actual content. It also ensures that the entire WordPress domain is not blocked just because a single blogger posts inappropriate content.

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	🟩	Users can be grouped in whatever way is required, and policy can be applied to different groups to vary filtering strength or type of content. Age based groups could be configured alongside role- based, and users may belong to multiple groups.

● 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.	🟩	The FortiGate URL Web Filtering has a Proxy Avoidance Category that can be set to block, this will block Web Sites that offer browser based circumvention services, but in addition the FortiGate Application Control feature has the ability to block applications in the Proxy category which covers VPN proxy avoidance type features, there are over 197 known VPN proxy applications blocked currently and the live dynamic FortiGuard signature updates add new apps as they are discovered. Also under application control it is possible to identify and block DNS over HTTPS and DNS over TLS.
● 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	🟩	There are very flexible override possibilities allowing individual URLs, or groups of URLs (specified by patterns) to be blocked or passed, or to be re-assigned to a specific category, overriding the Fortinet category rating. There is also the possibility for the administrator to define custom categories. All config changes are logged against the user who made the change for audit purpose.

● 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.	🟩	Content filtering can be enabled to block text based content present on a page. Content filters need to be populated with the text elements to be blocked based on regex or wildcard statements. Application and webfilter profiles can be used to control which AI engines can be used.
● 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	🟩	Fortinet can provide an array of filtering solutions, at the device level we can provide FortiClient which can provide a local webfiltering capability applied to the device and user of that device no matter if they are on-prem or offprem. The FortiGate is used to provide a network level of filtering which typically is applied when the device is on-prem. Cloud based filtering can be provided in a number of ways one of which is a FortiGate hosted on a public cloud platform which is used to provide network level filtering. But typically the use of FortiSASE which can provide cloud based filtering under the control of the subscriber. The on-prem FortiGate the public cloud FortiGate and the FortiSASE can provide category based DNS filtering in addition to Web filtering and Application control.

● 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	🟩	Fortinet approaches web filtering differently for three broad areas: - **Malicious content**. This includes viruses and sites which are capable of exploiting vulnerabilities in users' browsers and other applications. Often these sites will be legitimate sites which have been compromised by a cybercriminal. The approach to detecting such sites is very different from general categorisation, since the visible content of the site provides no clues of the malicious content hidden within. - **Offensive content**. This includes such categories as pornography, violence and extremism, and are considered to be the categories which must be prioritised in terms of coverage and accuracy. As a result, a disproportionate amount of effort is given to rating these categories, in terms of human resources, research and development of automation tools, and ongoing daily processing. - **General content**. This includes such categories as shopping, news, sport etc, where ambiguities in rating can be tolerated. The goal of separating these groups is to ensure that the areas which represent the greatest risk are those for which Fortinet applies the highest priority.

	🟩	For the question of overblocking, care is taken to block on complete URLs wherever possible, rather than blocking based on a domain name or IP address. This approach allows a site to continue to function even if it contains malicious content, since only that content will be blocked, rather than the entire site being blocked because of one file. Note however that when a malicious file is identified on a given website, crawlers will be dispatched to try to identify any other malicious content which may be hidden in the same site. However, sometimes it is appropriate to give a single categorisation to an entire domain, so a hierarchical search is used to allow entire subdomains or paths within a site to be blocked if necessary. This applies also to user defined URL patterns.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	FortiManager is a central management platform that can perform policy management across multiple FortiGate units and give an oversight of logs, events, and generate reports using the FortiAnalyzer features.
● 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.	🟩	Users can be identified either by an explicit login to the system, or using the Fortinet single sign-on capabilities, in which a user can be identified from an authentication with the existing Active Directory or

	🟩	LDAP system. There are multiple ways to identify users and devices. Mobile devices could be forced to authenticate using captive portal or SAML authentication. It is also possible to identify users by RADIUS accounting if they sign on to the wireless network using username and password. Device identification can be enabled on the FortiGate to help ascertain the details of specific devices other than just IP address. User filtering policy can be as granular as per user but typically it is better to group users by typically their LDAP group or groups and use that group or groups as an identification source to apply the correct filtering policy.

● 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	🟩	The Fortinet FortiGate is a Next Generation Firewall (NGFW) that is Layer 7 Application aware, giving it the ability via its Application Control feature to control over 3200 applications in real time by identifying the traffic signature of the Application not just the Layer 3 & 4 IP and TCP/UDP ports used by the Application. New Application identification signatures are updated dynamically from the FortiGuard Labs and can be pushed to the FortiGate instantly without loss in service. Applications are grouped into 18 Different Categories such as Social Media, Gaming, P2P File Sharing, Proxy Avoidance, Storage & Backup, and Email. Granular policies can be set to control Applications individually or via the complete category, and then differing application control profile scan be applied to different set of users, such a staff or students. In conjunction with the SSL Inspection facility on the FortiGate further fine grained Application control can be achieved within some Applications such as disabling videos from playing within Facebook. Mobile apps can be controlled with application control but SSL deep inspection is important to enable greater control.

● Multiple language support – the ability for the system to manage relevant languages	🟩	The Fortinet web filtering system has inherent multi-language support where each language has an extensive dictionary which is used by the rating system to categorise content. The human web filtering team has fluency in over 15 languages
● 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	🟩	Fortinet can protect school-owned off-site devices with an endpoint agent installed in the following ways. FortiSASE™ – Cloud delivered security inspection. This is available for managed devices (FortiSASE agent) or unmanaged devices (Secure Web Gateway). The latter is particularly suitable for providing webfiltering security to Chromebooks. FortiClient™ can provide local protection or enforce a VPN connection with centralised protection. Logs from FortiClient will be uploaded automatically for reporting and alerting. FortiClient™ can synchronize webfilter policy with the FortiGate™ for a seamless approach either on premise or remote working.

● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	Reporting of URLs can be done via a number of means: - from the fortiguard.com web site - through Fortinet customer Support - through a form built into the default replacement page which is presented to a user who tries to access blocked content. Note that all requests received from any of these means are treated by a human team, not by automated rating systems.
● Reports – the system offers clear granular historical information on the websites users have accessed or attempted to access	🟩	Any category (including those which are overridden by the system administrator) can be optionally logged when there is a detection. Logs can be stored locally on the FortiGate device, or sent to FortiAnalyzer, our log storage and analysis solution, or simply sent using syslog to any third party log server. The FortiGate firewall can enforce safe search on web browser search requests. Safe search can also be enforced on FortiClient webfiltering for remote or off site users. There are default reports on FortiAnalyzer which can be
	🟩	run and filtered to particular users, these reports can have time and date scopes set to for historical usage to be shown in the report. These reports can also be scheduled and delivered via email in a format such as PDF.

● Safe Search – the ability to enforce 'safe search' when using search engines	🟩	The FortiGate firewall can enforce safe search on web browser search requests. Safe search can also be enforced on FortiClient webfiltering for remote or off site users.
● Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity	🟩	Fortinet can provide a webhook connection to a third party system to convey information which maybe relative to safeguarding events. FortiAnalyzer offers the ability to alert on the basis of types of words used in elements such as search terms or in conversations on social media applications such as Facebook. The usage of these words can be captured and reported in the default safeguarding report and delivered to a nominated safeguarding lead, there are also two additional reports available which provide for self harm word usage and bullying and offensive words usage. The alerting element for safeguarding can sent via email or MS Teams via a connector.

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.

Fortinet category based web filtering has a specific category for AI identified sites, there is also application identification and control available to allow or restrict access to certain GenAI applications. In terms of access control this can be achieved by identifying user groups by integration of the FortiGate into an IDP source typically LDAP/AD. User groups can be used in policy to identify the source and then provide restrictions on user access using a combination of web filtering and application control, currently there are more than 20 plus identified GenAI applications. Identifying the user/group can then be used to classify the access based on age / risk / or educational need. Content filters can be used in the web filtering profile to limit the returned content. FortiGuard threat intelligence provide an online resource to allow the submission of web sites or applications for reclassification. In terms of configuration guidance the docs.fortinet.com web site contains admin guides to help configure the FortiGate, there is also the community.fortinet.com where you can submit questions for help or search for information and guidance.

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

Fortinet offer a service called **Security Awareness Training** which is free to primary and secondary schools in the UK, and provides training on how to be safer and more aware online. Details of the security awareness training can be found at the following URL https://www.fortinet.com/training/security-awareness-training/education-edition-uk

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

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

- 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 selfcertification 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 supply all reasonable clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Ben Wilson
Position	SVP, Product Management
Date	2/24/2026
Signature	Signed by: FC441A1E53EC4CC...

Approved for Legal Terms Only

EDP

February 2026

Business Owner Responsible for Engagement and Business Terms