Appropriate Monitoring for Schools

May 2025

Monitoring 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 monitoring providers to illustrate to schools how their particular technology system(s) meets the national defined 'appropriate monitoring' standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is 'appropriate' for them.

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
Monitoring System	FortiGuard Web Content Monitoring
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.	

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
● Are IWF members		Fortinet subscribe to and are members of the IWF
● Utilisation of IWF URL list for the attempted access of known child abuse images		Fortinet include the URL list supplied by the IWF in our category-based webfiltering under the category of **Child Sexual Abuse**. This list is dynamically and centrally updated via FortiGuard services. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on.
● Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Fortinet include the URL list supplied by the CTIRU in our category-based webfiltering under the category of **Terrorism**. This list is dynamically and centrally updated via FortiGuard services. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on.
● Confirm that monitoring for illegal content cannot be disabled by anyone (including any system administrator) at the school		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.

Illegal Online Content

Monitoring providers should both confirm, and describe how, their system monitors/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.		**Category – Child Sexual Abuse** This category contains sites that have been verified by the Internet Watch Foundation to contain or distribute images of non-adult children that are depicted in a state of abuse. Information on the Internet Watch Foundation is available at https://www.iwf.org.uk/ Any attempts to access a URL within this category can be blocked, logged and reported/alerted on.

controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.		**Category – Explicit Violence** This category contains sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on. Any sites that have not yet been rated will be caught by the **Unrated** category for blocking, logging and reporting/alerting purposes.
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.		**Category – Explicit Violence** This category contains sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc.

			Any attempts to access a URL within this category can be blocked, logged and reported/alerted on. Any sites that have not yet been rated will be caught by the **Unrated** category for blocking, logging and reporting/alerting purposes.

extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.		**Category – Explicit Violence** This category contains sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on. Any sites that have not yet been rated will be caught by the **Unrated** category for blocking, logging and reporting/alerting purposes.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.		**Category – Illegal or Unethical** This category contains sites that feature information, methods, or instructions on fraudulent actions or unlawful conduct (non-violent) such as scams, counterfeiting, tax evasion, petty theft, blackmail, etc. **Category – Phishing** This category contains counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users. Any attempts to access a URL within these categories can be blocked, logged and reported/alerted on.

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.		**Category – Discrimination** This category contains sites that promote the identification of racial groups, the denigration of subjection of groups, or the superiority of any group. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.		**Category – Explicit Violence** This category contains sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. **Category – Terrorism** This category contains sites that depict 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. Any attempts to access a URL within these categories can be blocked, logged and reported/alerted on.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.		**Category – Illegal or Unethical** This category contains sites that feature information, methods, or instructions on fraudulent actions or unlawful conduct (non-violent) such as scams, counterfeiting, tax evasion, petty theft, blackmail, etc. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on.

promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide,		**Category – Explicit Violence**

	posing serious risks to vulnerable populations.		This category contains sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on. Any sites that have not yet been rated will be caught by the **Unrated** category for blocking, logging and reporting/alerting purposes.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.		**Category – Pornography** This category contains mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite. **Category – Other Adult Materials** This category contains 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. **Category – Nudity and Risque** This category contains mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse. Any attempts to access a URL within these categories can be blocked, logged and reported/alerted on.

selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.		**Category – Drug Abuse** Websites that feature information on illegal drug activities including drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc. **Category – Weapons (Sales)** This category contains sites that feature the legal promotion or sale of weapons such as hand guns, knives, rifles, explosives, etc. Any attempts to access a URL within these categories can be blocked, logged and reported/alerted on.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.		**Category – Pornography** This category contains mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite. **Category – Other Adult Materials** This category contains 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. Any attempts to access a URL within these categories can be blocked, logged and reported/alerted on.

Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.		**Category – Terrorism** This category contains sites that depict 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. Any attempts to access a URL within this category can be
			blocked, logged and reported/alerted on.

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Gambling	Enables gambling		**Category – Gambling** Sites that cater to gambling activities such as betting, lotteries, casinos, including gaming information, instruction, and statistics. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on.

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.		**Category – Explicit Violence** This category contains sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on. Any sites that have not yet been rated will be caught by the **Unrated** category for blocking, logging and reporting/alerting purposes.
Hate speech / Discrimination	Content that expresses hate or encourages violence towards a person or group based on something such as race, religion, sex, or sexual orientation. . Promotes the unjust or prejudicial treatment of people with protected characteristics listed in the Equality Act 2010		**Category – Discrimination** This category contains sites that promote the identification of racial groups, the denigration of subjection of groups, or the superiority of any group. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on.

Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content, including ransomware and viruses		**Category – Malicious Websites** This category contains 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. **Category – Hacking** This category contains sites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites. Any attempts to access a URL within these categories can be blocked, logged and reported/alerted on.

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		**Category – Alternative Beliefs** This category contains sites 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. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on. Any sites that have not yet been rated will be caught by the
			Unrated category for blocking, logging and reporting/alerting purposes.
Pornography	displays sexual acts or explicit images		**Category – Pornography** This category contains mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on.

Self Harm and eating disorders	encourages, promotes, or provides instructions for self harm or eating disorders		**Category – Explicit Violence** This category contains sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on. Any sites that have not yet been rated will be caught by the **Unrated** category for blocking, logging and reporting/alerting purposes.
VAWG	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.		**Category – Explicit Violence** This category contains sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. Any attempts to access a URL within this category can be blocked, logged and reported/alerted on. Any sites that have not yet been rated will be caught by the **Unrated** category for blocking, logging and reporting/alerting purposes.

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

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

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
• Age appropriate – includes the ability to implement variable monitoring appropriate to age and vulnerability. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community based access		Users can be grouped in any way that is required, including age-based, with users potentially belonging to multiple groups. Alerts can then be created based on these groups and/or relevant web filter categories to ensure that they are age/vulnerability appropriate.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Event handlers can be used on the reporting platform for alert management. Additionally, the reporting platform provides an incident management capability alongside the ability to

		communicate alerts via fabric/API connectors to third party systems.
• Audit – Any changes to the monitoring system are logged enabling an audit trail that ensures transparency and that individuals are not able to make unilateral changes.		All Fortinet products involved with web traffic monitoring automatically log any changes made to the system. These logs can then be sent to a log analysis tool, such as FortiAnalyzer™, for the generation of alerts when certain actions have been performed and reporting on any actions performed.
• BYOD (Bring Your Own Device) – if adopted by the school and the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location		Fortinet can monitor all destinations users visit on BYOD devices and log them for further analysis. When combined with FortiAuthenticator's SmartConnect function this monitoring is extended, allowing BYOD devices to be monitored as if they were school owned devices. Please note that the above only applies to onsite devices. The monitoring of devices off the school premises requires an endpoint agent (FortiClient) to be installed on the device.

● Data retention –what data is stored, where is it (physically– ie cloud/school infrastructure) stored and for how long. This should also include any data backup provision		All web access (as well as any security events such as malware or intrusion detections) can be logged (generally to a centralised customer owned log server) where log retention is under the complete control of the user. The data stored includes user ID (assuming that
		users are individually authenticated), URL visited, the ID of the security device which handled the transaction, as well as low-level addressing information and a timestamp.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		Client Software is not necessary to monitor devices when on School Premises and connected to the school network via Wired or Wireless. Client software is only required if Monitoring and Filtering is required when 'off network'. This is in the form of FortiClient™ software and is available for the following operation systems: • Windows Desktop • MacOS • iOS • Android • Chromebook

• Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy		The Fortinet web filter allows complete freedom to add, modify and remove keywords to be checked in web pages. Wildcard matches can be used for more flexible searching and thresholds can be applied to block only if a certain word appears multiple times.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Fortinet provides a centralized management platform to allow policy to be consistent across multiple locations. The centralized reporting platform also provides for consolidated or, if preferred, autonomous reporting for the multiple locations.
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (e.g. Image hash).		Currently, image reputation is done via their URL. There is no analysis of the images themselves.
• Identification - the monitoring system should identify users and devices to attribute activity (particularly for mobile devices) and ensure the application of appropriate configurations for individual users.		The Fortinet solution can identify individual users in a number of ways, with the primary method being via FortiAuthenticator. FortiAuthenticator is a powerful centralised authentication tool that is capable of providing transparent sign-on for school-owned devices, alongside tracking for BYOD devices (including onboarding methodologies).

• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		In general, such communication would be done via training or security awareness sessions. Note that if a user is blocked after accessing a website which belongs to a blocked category, a customisable block page will be displayed which can contain an explanation for the block, as well as information on whom to contact for more information, or a link to a support website.
• 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 monitoring system operate across mobile devices and app content. Providers should be clear about the capability of their monitoring system to monitor content on mobile and web apps and any configuration or component requirements to achieve this.		The Fortinet solution is entirely agnostic to the type of content being delivered for on-site devices. All traffic is identified and logged appropriately with no additional configuration for different content types. Off-site devices using FortiClient can have their traffic brought back to site for inspection via the FortiGate (content type agnostic) or locally filtered on the device itself. In the latter case, the traffic being filtered is determined by what the operating system allows FortiClient to filter.

• Multiple language support – the ability for the system to manage relevant languages?		The Fortinet web filtering solution is completely multilingual, both in the automated rating system, used for the majority of website rating, as well as for the human rating team which contains skills in all major languages to allow for detailed verification of page ratings.
• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?		Any blocked access will generate a log message, which may also generate an alert. A log analysis tool, such as FortiAnalyzer™, can generate alerts based on these logs. Such alerts may be generated for blocked URLs, or rules can be specified to limit alerts to specific categories or individual users or groups of users, or even a time of day. The alerts can then be sent by a number of means including email, SMS, SNMP traps.
• Remote monitoring – with many children and staff working remotely, the ability, extent and management for the monitoring of devices		Fortinet can protect school-owned off-site devices with an endpoint

(school and/or personal). Included here is the hours of operation together with the explicit awareness of users. Monitoring should focus on school-owned and managed devices. When shared devices are used, schools must ensure users log in individually. This allows monitoring systems to apply restrictions and configurations based on user profiles, improving the safeguarding process.		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 – how alerts are recorded within the system?		All detections of forbidden or suspicious accesses will be logged, either locally in the FortiGate (for very small installations) or to a centralised log manager, such as FortiAnalyzer.

• 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.

Pro Active Monitoring - how any pro-active monitoring support is provided including if any automation is utilised and the safeguarding capability of the organisation's teams.

Fortinet can provide pro-active monitoring in two ways.

1. Scheduled reports – FortiAnalyzer can be used to ingest log feeds from a multitude of Fortinet and third-party products, and provide scheduled reports to DSLs on user activity from that data.

2. Alerting – During the ingestion of logs, described above, FortiAnalyzer can send an alert to DSLs based off a multitude of criteria. For example, attempts to access blocked websites (individual attempts or multiple attempts in a given timeframe), attempts to use certain applications or applications of a certain type to evade the monitoring platform, searching specific words/phrases in a search engine, etc.

Please note below opportunities or enhancements to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

How does your monitoring system identify and respond to activity involving Generative AI technologies (e.g. AI prompts, content creation, or platform use)?

In your response, please explain how your system captures or analyses user interactions with Generative AI tools; to what extent logs or alerts reflect potential safeguarding risks associated with AI-generated content (such as harmful prompts or inappropriate use of image and text generation); any known limitations—whether technical, privacy-related, or device-specific—that may affect your system's ability to monitor such activity; and what guidance you provide to schools to support their understanding and management of Generative AI-related risks.

Fortinet provides a dedicated web filtering category for AI identified sites, alongside application identification and control to allow or restrict access to certain GenAI applications.

Access control for these applications/sites can be achieved by identifying users and their respective user groups through an integration of FortiGate into an IdP source; typically LDAP/AD or FortiAuthenticator. These user groups can then be used within policy to enforce restrictions on user access via a combination of web filtering and application control (currently more than twenty identified GenAI applications), based on the user's age, risk and/or educational needs.

All access (successful or not) to these sites and applications is logged for use within alerts and reports.

For configuration guidance, the https://docs.fortinet.com website contains admin guides to help configure various Fortinet products, and the https://community.fortinet.com website allows for users to submit questions for help or search for information/guidance.

MONITORING 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 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...