Appropriate Filtering for Education settings

June 2021

Filtering Provider Checklist Reponses

Schools 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, 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 they "should be doing all that they reasonably can to limit children's exposure to the above 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."

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to "have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content."

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	Forcepoint
Address	420 Thames Valley Park Reading Berks RG6 1PT England
Contact details	Donal O'Callaghan donal.ocallaghan@forcepoint.com
Filtering System	Forcepoint Web Security, Forcepoint Cloud Security Gateway
Date of assessment	10th November 2021

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	🟩	Can be found athttps://iwf.org.uk/become-a-member/join-us/our-members
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)	🟩	The IWF URL list is included into Forcepoint's URL Database which is the basis of the filtering provided by Forcepoint
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	Forcepoint includes the CITRU URL list into Forcepoint's URL database.

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
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.	🟩	Covered by the 'Intolerance' category. See Forcepoint URL Categories under 'Baseline Categories'
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	Covered by the 'Abused Drugs' category that is also included in the parent category 'Drugs' See Forcepoint URL Categories
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	Covered by the 'Militancy and Extremist' category See Forcepoint URL Categories

Content	Explanatory notes – Content that:	Rating	Explanation
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	🟩	Malware is addressed by a number of categories ‘Advanced Malware Command and Control’, ‘Advanced Malware Payloads’ & ‘Mobile Malware’ under the parent category of ‘Forcepoint Security Filtering’. Hacking is a separate category under the ‘Information Technology’ parent category. See Forcepoint URL Categories
Pornography	displays sexual acts or explicit images	🟩	Generally addressed as part of the ‘Adult Material’ parent category. Several child categories are provided including ‘Adult Content’, ‘Nudity’ and ‘Sex’ See Forcepoint URL Categories under ‘Baseline Categories’
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	Covered by the Hacking category under the ‘Information Technology’ parent category. See Forcepoint URL Categories under ‘Baseline Categories’
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	🟩	Covered by the ‘Violence’ category. See Forcepoint URL Categories under ‘Baseline Categories’
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	Covered by the ‘Violence’ category. See Forcepoint URL Categories under ‘Baseline Categories’

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

Forcepoint’s URL Database allows the categorization of Internet Content to enable School’s and other organizations to effectively implement acceptable use policies that are in line with that organizations needs and desires for their user population.
Forcepoint uses a combination of static categorization URL database and real-time content classification to ensure the efficacy of the categorization applied. Forcepoint’s URL Database and content categorization is continually updated as part of the Forcepoint Security Cloud.
Forcepoint ingest several external feeds including the IWF, CITRU as part of the generation and maintenance of the Forcepoint URL Database. This ingestion and generation is a fully automated process ensuring that Forcepoint’s URL Database is always up to date.

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 .

The standard retention policy is 90 days. Customers can control whether user identification and IP address information are logged. The solution is GDPR compliant and how personal data is managed is documented here

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

Forcepoint uses a combination of static categorization URL database and real-time content classification to ensure the efficacy of the categorization applied. Forcepoint’s URL Database and content categorization is continually updated as part of the Forcepoint Security Cloud. Customers can also request re-categorization if they disagree with the Forcepoint assigned categorization.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
● Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role	🟩	The solution allows the definition of separate policies such that each policy contains different filtering strengths. A Policy can then be assigned to one or more users and or user groups. In this case filtering can be varied based on age or role.
● Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.	🟩	The solution is a proxy based solution and will only process HTTP and HTTPs. VPN (IPSec) can typically be easily blocked by the premise based equipment used by the school to forward the traffic to Forcepoint’s security cloud.

	🟩	Forcepoint’s Web Security can ten block the listed circumvention methods over Web.
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content	🟩	Schools have the ability to define their own policies. Schools can also define and manage their own bypass lists and in this way further tailor the filtering applied to their needs.
● Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked. For example, being able to contextually analyse text on a page and dynamically filter	🟩	Forcepoint Web Security applies both real-time-content-classification (RTCC) and real-time-security-classification (RTSS) as content is streamed through the service to the end-user. RTCC and RTSS is applied to ensure the efficacy of the static categorization which is taken from Forcepoint’s URL Database
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	Forcepoint publicly publishes a list of all the categorisations and what they mean. Forcepoint also publicly publishes a whitepaper on the ACE Detection engine, outlining the different capabilities and approaches to detection that are used in the filtering product.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	The solution supports 1 or more policies. Policy can be assigned at a site, user, user group or combination thereof. Policies are managed centrally through the Forcepoint Admin Portal. This is a web interfaces hosted in Forcepoint’s Cloud and accessible on the public internet. The Web Portal also provides central oversight, dashboarding and reporting capabilities

● Identification - the filtering system should have the ability to identify users	🟩	Yes, users can be identified. Different identification methods are also supported include NTLMID and SAML based Single Sign-On
● 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)	🟩	Mobile endpoints that access the Internet through the site based connection will be subject to the assigned filtering policy and in this case inappropriate content will be blocked in the usual fashion. Please note the solution does not support deployment to mobile endpoints i.e. a mobile app is not provided.
● Multiple language support – the ability for the system to manage relevant languages	🟩	End User Notification including block pages and coaching pages can be configured and support different languages.
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)	🟩	Filtering can be applied on the Network Level. It can be applied based on Egress IP or if connected via a GRE/IPSec tunnel then filtering can be applied to the entire tunnel (i.e. a single policy for the entire tunnel) or to site specific subnets within that tunnel (i.e. different policy based on site subnet)
● Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school	🟩	The solution supports an endpoint client which can provide staff working remotely with the same level of filtering. An endpoint is provided for Windows and macOS.
● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	The solution includes reporting. This includes off the shelf or pre-canned reports, the ability to define custom reports and the ability to query transaction logs.

● Reports – the system offers clear historical information on the websites visited by your users	🟩	The solution includes historical reporting.

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

Forcepoint do not provide specific materials in this case. We do provide materials that could be incorporated as part of a wider curriculum but this would be based on the school itself leveraging relevant information published as part of Forcepoint's Security labs blog https://www.forcepoint.com/blog/x-labs.

Although this material is not specifically focused on education it does provide a broad insight into the overall threat landscape. This would not be suitable for primary level but could be relevant for secondary, further education and Higher Education particularly if the intent is to deliver a more detailed look at the threat landscape. Again this would only be as part of a wider curriculum and would require the educator to select the relevant information from this resource on a case by case basis.

[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	Donal O'Callaghan
Position	Product Management
Date	27th October 2021
Signature	