# Appropriate Filtering for Education settings

## June 2016

## 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*"[1]. Furthermore, the Department for Education published the revised statutory guidance 'Keeping Children Safe in Education'[2] in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated to "*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges 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 | Atom IT Solutions Ltd |
| Address | Rufford Court, Wellow Road, Eakring, Nottinghamshire, NG22 0DF |
| Contact details | 0800 9078609 |
| Filtering System | Fortiguard Web Control Filtering |
| Date of assessment | 3/1/2017 |

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. | |

.

[1] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

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

## 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 is a member |
| • and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list) | | The IWF list is part of Fortiguard Web Filtering Service.<br><br>Category – Child Abuse Websites 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 http://www.iwf.org.uk/. |
| • Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' | | The list is part of Fortiguard Web Filtering Service. |

## 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. | | Category - Discrimination Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group. |
| Drugs / Substance abuse | displays or promotes the illegal use of drugs or substances | | Category – Drug Abuse Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc |
| Extremism | promotes terrorism and terrorist ideologies, violence or intolerance | | Category - Extremist Groups Sites that feature radical militia groups or movements with aggressive antigovernment convictions or beliefs. |
| Malware / Hacking | promotes the compromising of systems including anonymous | | Category - Malicious Websites Sites that host software that is |

| | | | |
|---|---|---|---|
| | browsing and other filter bypass tools as well as sites hosting malicious content | | 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.<br>Category - Hacking Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites. |
| Pornography | displays sexual acts or explicit images | | Category – Pornography<br>Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite.<br><br>Category - Nudity and Risque<br>Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse. |
| Piracy and copyright theft | includes illegal provision of copyrighted material | | Category - Peer-to-peer<br>File Sharing Websites that allow users to share files and data storage between each other. |
| Self Harm | promotes or displays deliberate self harm (including suicide and eating disorders) | | Category - Explicit Violence<br>This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. |
| Violence | Displays or promotes the use of physical force intended to hurt or kill | | Category - Explicit Violence This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. |

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 by Fortinet and which has evolved over more than 13 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, managed by Fortinet, to be rated based on hit count and the current charge on the system. |

Atom IT Solutions Ltd manage the adding and removing of sites from blocked or allowed categories as part of our service.

Individual requests are received from approved users. These requests can be received via the block page forms or via our normal support channels 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 managed by Atom IT solutions in communication with the school.

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 |
|---|---|---|
| • Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role | | Atom IT integrates the Fortiguard Web Filtering system with the school's Microsoft Active Directory to create staff and pupil groups. Users can also be grouped in whatever way is required, and policies can be applied to different groups to vary filtering strength or type of content. Age based groups are created alongside role based, and users may belong to multiple groups. |
| • Control - has the ability and ease of use that allows schools to control the filter themselves | | There are very flexible override possibilities |

| | | |
|---|---|---|
| to permit or deny access to specific content | | 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. Atom IT Solutions Ltd employ the use of custom categories and to allow schools to categorise URL's to these custom categories. |
| ● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking | | Fortinet approaches web filtering differently for three broad areas: -<br><br>Malicious content<br>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.<br><br>Offensive content<br>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.<br><br>General content<br>This includes such categories as shopping, news, sport etc, where ambiguities in rating can be tolerated.<br><br>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.<br><br>For the question of over-blocking, 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 web site, crawlers will be dispatched to try to identify any other malicious content which may be hidden in the same site.<br><br>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. |
| ● Identification - the filtering system should have the ability to identify users | | Users are 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. |
| ● Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies | | Fortinet has a full range of security components including Application Detection which enables malicious or inappropriate mobile applications and content to be identified and blocked. |
| ● 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. |
| ● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices | | The FortiGate UTM firewall provides web filtering at the network level. |
| ● Reporting mechanism – the ability to report inappropriate content for access or blocking | | Reporting of URL's can be made through a form built into the Atom IT Solutions Ltd designed replacement page which is presented when a user tries to access blocked content. |
| ● Reports – the system offers clear historical information on the websites visited by your | | All blocked categories detections are reported |

| | | |
|---|---|---|
| users | | with user, via active directory integration, and timestamp details and logged to either FortiAnalyzer or Microsoft's Log Analytics depending on the Atom IT Solutions Ltd solution that is in place. Reports are presented back to the school safeguarding team through Microsoft Office 365 Power Bi. Reports are also split into specific KCSIE (keeping children safe in education) high importance categories. |

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[3]

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

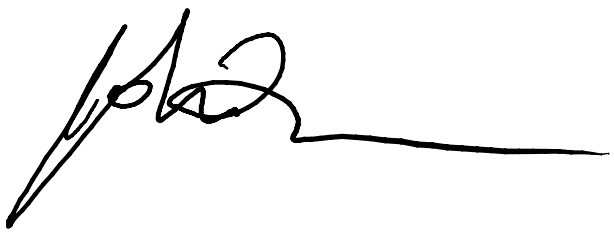
| |
|---|
| Information about staying safe online can be integrated into the blocking to inappropriate content, so rather than just blocking a page, information or a redirect is used to present information about educating students about online safety or any other topic.<br><br>Schools can also manage their own URL override settings if requested with training provided. |

[3] 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 | John Brown |
| Position | Director |
| Date | 03/01/2017 |
| Signature |  |