Appropriate Filtering for Education settings

June 2018

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. 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."

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	Lancaster University Network Services Ltd
Address	ISS Building Lancaster University, Bailrigg, LA1 4WA
Contact details	info@luns.net.uk 01524 510 510
Filtering System	Fortigate Network Security
Date of assessment	19-10-2018

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		The Cumbriagfl web-filtering solutions use Fortinet filtering solutions. Fortinet are IWF members.
• 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. **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.
• 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.		The Fortiguard web filtering offers category based filtering which is updated and adjusted regularly via an automated subscription program. Categories blocked relevant to this content include: **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		As above. Categories blocked relevant to this content include: **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		As above. Categories blocked relevant to this content include: **Extremist Groups** Sites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		As above. Categories blocked relevant to this content include: **Malicious Websites** 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

Pornography	displays sexual acts or explicit images		As above. Categories blocked relevant to this content include: **Pornography** Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite. **Nudity and Risque** Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse and excite.
Piracy and copyright theft	includes illegal provision of copyrighted material		As above. Categories blocked relevant to this content include: **Peer-to-peer 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)		As above. Categories blocked relevant to this content include: **Explicit Violence** 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		As above. Categories blocked relevant to this content include: **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 in-house by Fortigate 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 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.

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

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. In addition to the filterlists management by Fortigate, CumbriaGfl retain the ability to manage custom 'black' and 'white' lists in the system based on our own review of sites and users requests.

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		As a centralised solution the CumbriaGFL filtering by default the filtering operates at a core level of standardised safe filtering for all users Differentiated filtering is achieved through integration between Fortigate and the institution's user identification system which is typically Windows AD. This can identify each individual user and apply appropriate levels of filtering.
• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services		FortiGuard maintains constantly updated lists of well-known proxy bypass sites/VPNs etc. All such sites are blocked by default.

• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Institutions may apply to reclassify incorrectly blocked content via a live online process, unblocking valid content in near realtime. Where access to a correctly policy blocked resource is required blocked application for an override can be logged with Cumbriagfl support and a list of institution based rules/exceptions to the default filtering may be compiled Institutions may elect to join a 'beta' program allowing a live, authenticated, override to block pages. This may be based on a institution level password or on integration with their own identity systems.

• 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: - 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 over-blocking, care is taken to block

• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		There is an administrative dashboard where global policy settings can only be applied by CumbriaGFL administrators and not overridden by any single institution.
• Identification - the filtering system should have the ability to identify users		Users are able to be identified in a number of ways. If the institution is using a directory service such as Windows AD Fortigate can integrate with this and identify a user for any given web session. Alternatively the user can be identified by cross-referencing the device IP address for a given web session with the device logs to ascertain who was logged in at the time.
• 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)		Fortinet has a full range of security components including Application Detection which enables malicious or inappropriate mobile applications and
• 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 CumbriaGfl filtering (by Fortinet) operates by default as an explicit proxy to allow for its implementation independent of an institutions Internet service provider. However institutions connected to our infrastructure directly or via VPN may elect to have transparent network level filtering.
● Reporting mechanism – the ability to report inappropriate content for access or blocking		Reporting of URLs can be done via a number of means: Reporting to the Cumbria Schools helpdesk directly for adding to our networks own blacklist sites, Or Directly to Fortigate via from the fortiguard.com web site.
● Reports – the system offers clear historical information on the websites visited by your users		All blocked and allowed traffic is logged. These logs can be made available to an institution on request.

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

[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	Miles Burke
Position	Operations Manager
Date	19-10-2018
Signature