# Appropriate Filtering for Education settings

## September 2019

## 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 | Opendium |
| Address | Highfield House<br>1 Brue Close<br>Bruton, Somerset<br>BA10 0HY<br>United Kingdom |
| Contact details | sales@opendium.com<br>01792-824568 |
| Filtering System | Opendium Web Gateway / Opendium UTM |
| Date of assessment | 18th September 2019 |

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 | | Opendium are IWF members. |
| • and block access to illegal Child Abuse Images (by actively implementing the IWF URL list) | | The IWF Child Abuse Image Content URL list is integrated into the *Child Abuse Images* filtering category and Opendium has successfully completed the IWF's certification process.<br><br>Opendium systems go beyond the basic protection by also utilising the IWF's keywords list, and Non-Pornographic Child Abuse Images URL lists.<br><br>As well as directly blocking content that the IWF has listed, all of these resources are also used to dynamically identify and block offending content which has not yet been reported to the IWF. |
| • Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' | | The police assessed list of unlawful terrorist content, produced on behalf of the Home Office is integrated into the *Radicalisation* filtering category. |

## 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. | | Opendium provides a *Discrimination* filtering category which covers content that promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.<br><br>A *Hate* filtering category is provided which covers content promoting religious or racial hate. |

| | | | |
|---|---|---|---|
| Drugs / Substance abuse | displays or promotes the illegal use of drugs or substances | | Opendium provides a *Drugs* filtering category which covers content that promotes or facilitates recreational drug use, including "legal highs". This category does not include educational material about recreational drugs and information about medicinal drugs. |
| Extremism | promotes terrorism and terrorist ideologies, violence or intolerance | | Opendium provides a *Radicalisation* filtering category which covers radicalisation, extremism and terrorism. This includes the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. |
| Malware / Hacking | promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content | | Opendium provides a *Cracking* filtering category which covers information about how to gain illicit entry to computer systems.<br><br>An *Anonymisers / Proxies / VPNs* filtering category is provided to control anonymous browsing systems which could be used to bypass filtering and monitoring. |
| Pornography | displays sexual acts or explicit images | | Opendium provides a *Pornography* filtering category which covers pornographic content. This does not include non-sexualised images (e.g. medical information).<br><br>A *Sexualised Text* filtering category is provided which covers textual content which is sexual in nature but falls short of being considered pornographic. |
| Piracy and copyright theft | includes illegal provision of copyrighted material | | Opendium provides a *Copyright Infringement* filtering category which covers content that promotes and facilitates illegal downloading of copyrighted content, such as software, music, |

| | | | |
|---|---|---|---|
| | | | movies, etc. |
| Self Harm | promotes or displays deliberate self harm (including suicide and eating disorders) | | Opendium provides a *Self Harm* filtering category which covers content that promotes self harm and suicide. |
| Violence | Displays or promotes the use of physical force intended to hurt or kill | | Opendium provides a *Violence* filtering category which covers content that promotes violent acts. |

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

A selection of predefined filtering categories are maintained by Opendium, and updates are downloaded every hour. Websites and web searches are automatically categorised using a variety of methods, including through a database of known web addresses and by real time content analysis. By analysing content on the fly, the system can effectively filter new content and websites that tailor dynamic content to the individual user, such as social networking sites. School system administrators can add filtering criteria to the filtering categories to either augment or override the predefined criteria. School administrators can also add their own custom filtering categories.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy.

***Opendium Web Gateway*** and ***Opendium UTM*** are available as both cloud based and on-premises systems. Cloud based systems store internet history data on Opendium's servers, whereas for the on-premises systems this data is stored on the school's server. In both cases, the school can specify a retention period after which the log file data will be automatically deleted.

Internet history data that is stored on Opendium's internal systems will be retained for no longer than 3 years. This includes any log extracts, reports, etc. that the school may need to send to the technical support team.

Opendium provides schools with a standard data processing agreement, which outlines the protection and responsibilities regarding the personal data that Opendium handles on behalf of the school.

Many filtering providers rely on contractual clauses that place an onus on schools to ensure that they do not pass on personal data to the provider. Opendium strongly believes that such restrictions get in the way of providing the level of support that schools expect, and ultimately result in the routine breaking of data protection laws, with the school carrying the liability. Opendium feels that all schools should have a suitable data processing agreement with the company that supports their filtering system, to ensure that personal data is always handled in a secure and legal way.

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

| |
|---|
| ***Opendium Web Gateway*** and ***Opendium UTM*** allow school administrators a lot of scope for tuning the system to meet their needs. The sensitivity of the filters can be adjusted and administrators can decide whether or not repeat offenders should have their web access automatically disabled. Miscategorised websites can be manually recategorised instantly, or the filters completely disabled for educational websites. Users can be given the option to override the filters after being shown a warning, and all users can report miscategorised pages directly to Opendium to be manually examined and recategorised. Comprehensive reports can be generated on an automatic or ad-hoc basis to ensure that staff can spot and follow up on concerning behaviour. Location based filtering is also included, which can be used to relax filters in supervised parts of the school.<br><br>Schools may decide that, for some categories, rather than risk overblocking it is better to allow access and to follow up concerning behaviour that is highlighted by the reporting system. A variety of reporting tools are provided to facilitate this, such as the unique *Word Cloud* report that flags up search phrases which fall into concerning categories. This provides an easy and understandable way for staff to drill down into the data. |

## 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 | | ***Opendium Web Gateway*** and ***Opendium UTM*** both integrate with the school's existing user directory and provide a hierarchical system to configure and refine filtering policies on a per-usergroup, per-network or per-user basis. |
| • 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. | | ***Opendium Web Gateway*** and ***Opendium UTM*** provide a variety of tools to prevent circumvention of the system:<br><br>Opendium provides an *Anonymisers / Proxies / VPNs* category to control anonymous browsing systems.<br><br>*Both* ***Opendium Web Gateway*** and ***Opendium UTM*** incorporate anti-spoofing technologies and |

| | | |
|---|---|---|
| | | utilise deep packet inspection to restrict VPN connections whilst allowing other applications. ***Opendium UTM*** provides additional protection by providing numerous firewall rule bundles which utilise deep packet inspection to prevent VPN connections misusing ports that are required by legitimate services.<br><br>Opendium's online safety systems do not rely on DNS filtering, so are unaffected by technologies such as DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT). ***Opendium UTM*** also performs DNS and NTP interception to prevent VPNs from taking advantage of these important ports without getting in the way of legitimate systems that rely on them.<br><br>New VPNs are appearing all of the time and use a wide variety of techniques to mask their traffic. It is important for schools to understand that no system can block them with 100% accuracy, but Opendium works closely with schools to rapidly provide a solution whenever a new threat is identified. |
| ● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content | | The web based user interface allows school administrators to adjust settings from anywhere in the school, with immediate effect. All Opendium customers have direct access to Opendium's experienced |

| | | |
|---|---|---|
| | | engineers, who endeavour to provide high quality telephone and email support. |
| • Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking | | Opendium's filtering rationale is described in the knowledgebase:<br><br>http://www.opendium.com/knowledgebase/filtering-rationale<br><br>A description for each filtering category, outlining the categorisation criteria, is provided through the system's user interface. |
| • Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard | | Opendium systems are designed for single-school installations and therefore do not require multi-site management. However, individual systems can be managed remotely from anywhere in the world.<br><br>We expect to provide a comprehensive multi-site management solution in the future. |
| • Identification - the filtering system should have the ability to identify users | | ***Opendium Web Gateway*** and ***Opendium UTM*** both support a variety of user identification methods, such as Kerberos single sign on for workstations and RADIUS accounting, WISPr and captive portal for mobile devices / BYOD. |
| • 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) | | By providing a comprehensive transparent proxy service with both passive and active HTTPS inspection and decryption, ***Opendium Web Gateway*** and ***Opendium UTM*** both allow the school to control |

| | | |
|---|---|---|
| | | apps that communicate using HTTP and HTTPS, and these comprise the vast majority of apps.<br><br>A minority of apps use entirely different delivery mechanisms, and ***Opendium Web Gateway*** provides a firewall that can control these on a per-network basis. ***Opendium UTM*** extends this capability to allow fine grained control over these apps by user group or individual user, in a similar way to web traffic. |
| • Multiple language support – the ability for the system to manage relevant languages | | The use of a wide variety of categorisation methods makes the system largely language agnostic, filtering both English language and foreign language websites alike.<br><br>Opendium's textual content analysis system uses unicode to support all languages and character sets. |
| • Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices | | ***Opendium Web Gateway*** and ***Opendium*** UTM both provide network level filtering and do not require software to be installed on user devices. This is provided through a combination of deep packet inspection, transparent proxying and both active HTTPS decryption and passive HTTPS inspection. |
| • Reporting mechanism – the ability to report inappropriate content for access or blocking | | When access to a website is blocked, the user is given an option to report a miscategorisation of the website directly to Opendium. All reported web |

| | | |
|---|---|---|
| | | sites are manually examined and, if necessary, recategorised.<br><br>Opendium also takes underblocking very seriously and welcome reports of such instances. Opendium continually works with customers to address any concerns and improve the accuracy of the filters. |
| • Reports – the system offers clear historical information on the websites visited by your users | | ***Opendium Web Gateway*** and ***Opendium UTM*** keep historical logs and can generate a variety of reports to allow staff to drill down into the data. |

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

| |
|---|
| Opendium's products have always been developed hand-in-hand with schools. Schools are on the front line and in the best position to know what tools they need and Opendium always tries to listen and develop those tools.<br><br>Opendium provide a holistic service which goes above and beyond filtering, This includes training and advice for school ICT and safeguarding staff, and consultancy services to improve schools' network infrastructure to cater for their ever changing requirements. However, Opendium will never pressure schools into purchasing additional services and are equally happy to work with third parties to bring about any infrastructure improvements that the schools require. |

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 | Stephen Hill |
| Position | Technical Director |
| Date | 18th September 2019 |
| Signature |  |