# Online Safety Filtering and Monitoring Policy

| | |
|---|---|
| Procedure Originator: | Dawn Platt |
| Approved By: | Executive Leadership Team |
| Date Approved: | September 2018 |
| Review Interval: | Three Years |
| Last Review Date | July 2021 |
| Next Review Date | July 2024 |
| Audience: | ALL |

## 1. Introduction

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" (Revised Prevent Duty Guidance: for England and Wales, 2015).

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 (e.g. www.360safe.org.uk ) that will support a school in assessing their wider online safety policy and practice.

The use of technology has also become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

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 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.”

Whilst internet filtering has always been provided by schools, it is the ‘strengthened measures’ that are now a key part of Ofsted online safety during inspections.

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.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty.

## 2. Aims and Objectives

Each academy within the trust will have its own unique demands and use of the internet. However, all academies must ensure they appropriately safeguard staff and pupils through an effective online filtering and monitoring regime.

## 3. Requirements of Online Filtering and Monitoring

All academies within the Trust must ensure that internet systems are robust and appropriate for use. Academies are required to follow the Trust guidance below.

**Shaw Education Trust Guidance**

The Shaw Education Trust require all schools to be able to demonstrate how their systems manage effective filtering and monitoring by the completion of an annual safety check, including filtering and monitoring. Shaw Education Trust will provide checklists/documentation for use in schools.[1] [Appendix A and Appendix B]

The completion of these checks will allow all leaders to construct a risk assessment that considers the risks that both children and staff may encounter online.

1[This detail has been developed by the South West Grid for Learning, as coordinators of the UK Safer Internet Centre, and in partnership and consultation with the 120 national '360 degree safe Online Safety Mark' assessors (www.360safe.org.uk) and the NEN Safeguarding group (www.nen.gov.uk).]

| Actions To Take by the School | Actions to take by Academy Councillors |
|---|---|
| Recommendation that an online self-review takes place. For example: www.360safe.org.uk | Check that the school has completed annual Online Safety Checks (Filtering and Monitoring) |
| Complete the annual online filtering and monitoring checks and return to the Shaw Education Trust | Check to see a risk assessment summary for children and staff is in place that satisfies the Prevent Duty |
| Complete a risk assessment that considers the outcomes of checks and limits the risks that children and staff may encounter online | |

## 4. Roles and Responsibilities

### 4.1 The Board of Trustees

The Board of Trustees has delegated the responsibility for monitoring the way in which online monitoring and filtering is implemented within each academy to the Executive Leadership Team and the Academy Councils.

### 4.2 Executive Leadership Team (ELT)

The ELT are responsible for monitoring the effectiveness of safeguarding within schools and making checks on the appropriateness of online filtering and monitoring systems in academies.

### 4.3 The Academy Council

The Academy Council will monitor the effectiveness of this policy and hold the headteacher/principal to account for its implementation. They should be doing all that they reasonably can to limit children's exposure to risks online risks through the school's IT system.

### 4.4 Headteacher or Principal

The headteacher/principal and appropriate senior leaders, are responsible for ensuring that this policy is adhered to, and that:

- Their school or college has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn.
- They consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.
- Leaders conduct a risk assessment as required by the Prevent Duty.
- The school keeps a breast of statutory changes of government policy, and that the school meets all legal requirements for online monitoring and filtering.
- The school implements the relevant statutory arrangements for online monitoring and filtering.

### 4.5 Other staff

Other staff will ensure that they follow school policy with regard to appropriate use of the internet and that they use the school reporting mechanisms to alert leaders to any breaches in filtering and monitoring systems.

## 5. Links with other policies

This policy will be monitored as part of the Trust's annual internal review and reviewed on a three year cycle or as required by legislature changes.

This policy links to the following policies and procedures:

- Staff Code of Conduct Policy
- Child Protection and Safeguarding Policy
- Prevent Duty Policy

# Appendix A - Provider Checklist for Filtering

| | |
|---|---|
| School | Fortis Academy |
| Name and contact details of Network Manager | Glyn Jones – Tel 0121 366 6611 ext 273 |
| Filtering System | Netsweeper |
| Date of assessment/checklist | 18/12/18 |

System rating response to use in the check boxes below:

| | |
|---|---|
| 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 | | Netsweeper is a long-time member supporting the IWF for over ten years, with council representation. |
| • and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list) | | The Netsweeper product integrates with the IWF CAIC illegal content list. The IWF functionality is not exposed in the web admin graphical user interface and cannot be disabled. Importantly, Netsweeper regularly submits URLs discovered by the global systems back to the IWF team, who review the material to decide on inclusion in future updates of the IWF listings. In addition, Netsweeper is also one of the first filtering companies to support the Image Hash List, delivering the most effective and efficient solution for combatting the circulation of child sexual abuse images online. Netsweeper ensures that child-abuse imagery which has previously been identified by the IWF will be identified using Microsoft PhotoDNA and blocked if it appears on a new URL. |

| | | |
|---|---|---|
| | | https://www.iwf.org.uk/news/netsweeper-and-iwf-up-ante-against-child-sexual-abuse-imagery-microsoft-photo-dna-technology |
| • Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' | | With access to the CTIRU, Netsweeper uses the UK Home office's terrorism blocklist to block terrorist content per Government guidelines. Netsweeper integrates the list into their worldwide 500 million user cloud delivery categorising new content and offering unmatched global protection against terrorist and extremist content. |

## 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. | | Netsweeper has a category called 'Hate Speech'. These sites portray views that are written, verbal, or illustrated, and are intentionally offensive to the general public. The intent of these sites are to degrade, intimidate, incite violence, prejudicial actions against individuals based on race, ethnic affiliation, nationality, gender, sexual orientation, religion, disability, or profession. Advocacy/instructional sites that promote the harming of individuals/groups and encourage/promote peer abuse, videos of physical assaults, written harassment and threats are also included. |
| Drugs / Substance abuse | displays or promotes the illegal use of drugs or substances. | | Netsweeper has a specific category named 'substance abuse' which is blocked. |

| | | | |
|---|---|---|---|
| | | | These sites provide information about or promote the use of prohibited, illegal, controlled, or regulated substances for recreational rather than medicinal use. It can include sites that sell, encourage or advocate the use of any substance that produces hallucinations, as well as the cultivation, manufacture, and distribution of any intoxicant and related paraphernalia. Informational sites that are clearly intended to provide descriptions of drugs and substances, their negative effects, and addiction potential are not included. |
| Extremism | -promotes terrorism and terrorist ideologies, violence or intolerance. | | Categories within Netsweeper that block this content include ‘Extreme’, ‘Hate Speech’, ‘Criminal Skills’ and ‘Weapons’. Definitions can be found below:<br><br>**Extreme**<br><br>This includes sites that are considered far from normal and are categorized for their degree of intensity. The content features or promotes intentional, direct, and deliberate violence and destruction or the alteration of the human body and other living creatures. These sites may depict/promote torture, self-inflicted harm, mutilation, or other dangerous activities. Images and information that |

| | | | |
|---|---|---|---|
| | | | advocate and glorify eating disorders, suicide, death, gore, injuries or sites that feature grotesque or frightening descriptions are also included.<br><br>**Hate Speech**<br><br>These sites portray views that are written, verbal, or illustrated, and are intentionally offensive to the general public. The intent of these sites is to degrade, intimidate, or incite violent or prejudicial actions against individuals based on race, ethnic affiliation, nationality, gender, sexual orientation, religion, disability, or profession. Advocacy or instructional sites that promote the harming of individuals or groups and encourage or promote peer abuse, videos of physical assaults, written harassment and threats are also included.<br><br>**Weapons**<br><br>This includes sites that provide information related to the promotion, support, sale, or discussion of weapons and any related device used in combat that can injure or kill, such as guns, knives, or swords. Information on how to build weapons or bombs will also be included in 'Criminal Skills'.<br><br>**Criminal Skills** |

| | | | |
|---|---|---|---|
| | | | This includes sites with instructions or methods that promote, encourage, or provide skills considered to be illegal, criminal, violent or harmful to the general public, and are forbidden by law. This can include questionable material and sites that promote nonviolent,unethical, or dishonest behaviour such as academic cheating, or software hacking/key breaking. This does not necessarily reflect the laws of any particular region or country. |
| Malware / Hacking | -promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content. | | Netsweeper has categories named ‘Malware’, ‘infected hosts’, ‘phishing’, ‘viruses’ and ‘adware’. These categories block websites sites that are associated with this. These are sites containing scripts, or code, that may be ran in a hostile or intrusive manner to a system. |
| Pornography | -displays sexual acts or explicit images. | | Netsweeper has a pornography’ category which contains URLs that reference, discuss, or display pornographic images, videos, or other sexually oriented material that is created for the purpose of arousing sexual interest. Soft and hard-core pornography, sadomasochism, bestiality, fetishes, erotic stories, adult magazines, sex toys, or any other sexual related products are included. |
| Piracy and copyright theft | -includes illegal provision of copyrighted material. | | Two distinct Netsweeper categories satisfy this requirement; i.e., “Criminal Skills” and Piracy. Criminal Skills includes sites with instructions or methods that promote, encourage, or provide skills considered to be |

| | | | |
|---|---|---|---|
| | | | illegal, criminal, violent or harmful to the general public, and are forbidden by law. This can include questionable material and sites that promote nonviolent, unethical, or dishonest behaviour such as academic cheating, copyright infringement or software hacking/key breaking. This category does not necessarily reflect the laws of any particular region or country. Piracy (Torrents included): includes sites that distribute software and facilitate the direct exchange of files between users. Software that enables file searching, sharing and transferring across a network independent of a central server as well as web based sites of this nature are included. |
| Self-Harm | -promotes or displays deliberate self-harm (including suicide and eating disorders). | | The Netsweeper “extreme” category blocks sites categorised as self-harm sites, anorexia, bulimia and other content that prove harmful to children. |
| Violence | -displays or promotes the use of physical force intended to hurt or kill. | | Violence sites are included in the extreme category which includes sites that are considered far from normal and are categorized for their degree of intensity. The content features or promotes intentional, direct, and deliberate violence and destruction or the alteration of the human body and other living creatures. These sites may depict or promote torture, self-inflicted harm, mutilation, or other dangerous activities. Images and information that advocate and glorify eating disorders, suicide, death, gore, injuries or sites that feature grotesque or frightening descriptions are also included. |

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

Netsweeper has provided filtering solutions to the UK Education market for over 18 years and is trusted to protect the networks of over 30% of schools in the United Kingdom. Offering a global collective community experience, Netsweeper resides in over 63 countries, is localised in 37 languages, has categorised over 10 billion URLS and is used to filter over 500 million devices worldwide. The web as we know it is consistently changing and by navigating to http://www.netsweeper.com/live-stats/ one can see in real time the new content Netsweeper is categorising each and every day.

The value we bring to our customers is the Netsweeper collective platform where our customers experience the peer-to-peer benefits of our premium Cloud based categorization capabilities; through an intuitive easy to use interface enabling educational administrators to effectively deal with illicit web content on their networks.

Netsweeper offers category based alerting meaning you can customise and create alerts to be sent to safeguarding members of staff, head teachers, IT personnel. This can be triggeredautomatically, so for example you can create a ‘Prevent’ Report as illustrated below.


In this example an alert has been triggered asthese 5 users have tried to access one of the Prevent categories Netsweeper has. You can then drill down and find what time the specific users accessed the content as well as their location.

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

| |
|---|
| Netsweeper defines policies based on the categorisation of URLs. Policies will generally denyselected categories. Policies also have override lists, if a URL would be denied by a category, thelists can be used to amend that decision to be allowed. For example: If the policy denies the 'Social Networks' category, but the administrator wishes to allow Facebook, a simple entry in the local list to allow facebook.com is all that is needed.<br>Users with administrative rights are able to modify their policy (categories and lists) according to their permissions. |

## 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 | | Netsweeper is integrated with an existing directory system such as Microsoft AD, Novell LDAP, Apple LDAP, OpenLDAP or Radius Accounting to assign users based on their group or attribute to the correct filtering policy. |
| • Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services | | Netsweeper's real time filtering ensure that all new proxy and VPN services are categorised and blocked on the fly. Please check out https://www.netsweeper.com/live-stats/ to see how many new proxy and VPN services have been categorised in the last 24 hours. |
| • Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content | | Netsweeper natively supports multiple tenancy and delegated administration with fine-grained permissions control. This control has two effects, it will simplify the web-admin graphical user interface removing elements of the interface that the user does not have permission for, and constraining the access to site data and policies. Nominated individuals will have delegated administration for clusters of sites, and/or individual sites. The ability to manage policies and lists, and report on the associated data will be provided. |
| • Filtering Policy – the filtering provider publishes a rationale that details their | | The Netsweeper collective community numbers over 500 million devices worldwide. This |

| | | |
|---|---|---|
| approach to filtering with classification and categorisation as well as over blocking | | collective together with our technology and human oversight defines URL classification.<br>Netsweeper publishes classification of filtering and categorises on the Netsweeper website as well as a view in real time of new content categorised. This can be found at either http://www.netsweeper.com or http://www.netsweeper.com/livestats<br>Netsweeper's core competency is using our patented techniques to categorise every URL that passes through our deployed systems. Netsweeper is both real-time and employ a hierarchy of data (URLto-category), with our Category Naming Service (CNS) as a globalmaster database.<br><br>If any customer anywhere in the world accesses a URL, that URL is submitted to the local policy server, if that policy server cannot find a category match, it is automatically submitted to the CNS and looked up there. If the CNS already has the category mapping it is immediately returned to the local system and cached there for future use, a policy decision is then made by the policy server.<br>If neither the local system, nor the CNS has a category match, the URL is submitted to our "Artificial Intelligence" system that will interrogate the content at-and around that URL, assess the content, detect if it references or contains malware, and assigns one or more categories to the URL into the CNS and then back to the local system, a policy decision is then made by the policy server. The CNS allows us to adapt to trending URLs immediately due to |

| | | |
|---|---|---|
| | | its world-wide scope. If the local system hasn't seen a particular URL yet, then CNS probably has.<br>If the URL has been assigned one or more categories, local systems see immediate responses (sub-second).<br>If the URL is truly "new" then the AI will typically process the content within 20 seconds.<br>The local policy servers can be configured with techniques to minimise the "new URL" wait. |
| • Identification - the filtering system should have the ability to identify users | | Netsweeper sits in the core of the network and configured to proxy all traffic. Netsweeper is integrated with an existing directory system such as Microsoft AD, Novell LDAP, Apple LDAP, OpenLDAP or Radius Accounting to assign users based on their group or attribute to the correct filtering policy. For guest/wireless networks Netsweeper can utilise Radius Accounting packets which are generated by the Wireless Access Controller to identify when a user has authenticated. No additional software or agents are required. |
| • 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) | | Netsweeper has a Packet Inspection System that can detect a variety of protocols using its unique outbound inspection system. Policies are defined based on ‘category’ which means that application protocols are ‘categories’ that can be turned off and on a per IP, per subnet, per group or global basis. Netsweeper can also be deployed as an SSL Decryption Proxy for applications that utilize HTTPS for its mobile applications further adding functionality to limit and control applications, such as limiting functionality on social network sites.<br>Furthermore Netsweeper provides specific grouping of |

| | | |
|---|---|---|
| | | Categories headed as "Web Apps". The PDF below highlights the current supported Web Apps (most of the categories are shown "collapsed", eBay, YouTube, Google, and Facebook are open. |
| ● Multiple language support – the ability for the system to manage relevant languages | | Importantly, Netsweeper can categorise pages not only in English, but also in multiple languages. Netsweeper currently supports the following languages for URL classification: Arabic, English, French, German, Japanese, Persian, Polish, Russian, Simplified Chinese, Spanish, Turkish and Vietnamese. Future releases will include: Somali, Bangla, Croatian, Estonian, Swedish, Irish, Norwegian, Thai, Bulgarian and Traditional Chinese. Netsweeper's web site has a live stats page which gives an overview of some of the categories and languages. (www.netsweeper.com/livestats/). As the popularity of a particular language increases, Netsweeper adds support for that language. |
| ● Network level - filtering should be applied at 'network level' i.e., not reliant on any software on user devices | | Netsweeper can be configured and deployed as an explicit proxy, transparent proxy, out of band (port mirroring), inline or DNS URL Filtering system. Netsweeper Policy servers are deployed at the Internet gateways and communicate with a cloud based Category Name Service (CNS) in order to provide near real-time updates for URL classifications. Policy decisions are enforced on a per user, per group or global basis with time of day filtering and allowed or denied list overwriting the cloud based classifications. |
| ● Reporting mechanism – the ability to report inappropriate content for access or blocking | | Reports can trigger emails, thus a scheduled report can be considered an alert if the report contains data (if the report contains no data take no action). |

| | | |
|---|---|---|
| ● Reports – the system offers clear historical information on the websites visited by your users | | Netsweeper provides a very flexible reporting tool. Out of the box a number of pre-defined quick reports are available, these can be adapted or removed as desired. Quick reports are typically graphical and provide visibility of for example “top 10 web sites” (there are many different quick reports)<br>The reporting tool has the concept of demand reports and scheduled reports.<br>Demand reports are typically oneoff reports for a specific demand. For example “Can you tell me what web sites were accessed today between 10am and noon?”<br>Scheduled reports run on a defined schedule. Scheduled reports are useful for informative info-graphics. For example, top 10 web sites visited this week, top 10 web sites denied this week.<br>Reports can be graphical (pie charts,<br>bar-charts), or detailed (tabular text), or combined. Graphical reports can be multi-layered, allowing for interactive<br>reports where further detail can be discovered by drilling down.<br>There are various export options (image, PDF, CSV, etc…) |

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]

# Appendix B - Provider Checklist for Monitoring

| | |
|---|---|
| School | Fortis Academy |
| Name and contact details of Network Manager | Glyn Jones – Tel 0121 366 6611 ext 273 |
| Filtering System | Smoothwall RADAR |
| Date of assessment/checklist | 18/12/18 |

System rating response to use in the check boxes below:

| | |
|---|---|
| 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 thei 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 | | Smoothwall are IWF members, and where appropriate, use IWF material to aid monitoring alerts |
| • Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' | | Smoothwall work with CITRU to improve the accuracy of our PREVENT alerting |

## 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 |
|---|---|---|---|
| Illegal | -is illegal, for example child abuse images and unlawful terrorist content. | | RADAR contains a variety of Safeguarding themes which pick up illegal content, including a theme specifically aimed at PREVENT. |
| Bullying | -involves the repeated use of force, threat or coercion | | Bullying takes many forms, and RADAR can pick up |

| | | | |
|---|---|---|---|
| | to abuse, intimidate or aggressively dominate others. | | bullying content in the “Racism and Violence” theme as well as others targeted at more general behaviour issues. |
| Child Sexual Exploitation | -encourages the child into a coercive/manipulative sexual relationship. This may include encouragement to meet. | | The “Predators and Strangers” theme is specifically designed to pick up this type of activity. |
| Discrimination | -promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity. | | The Racism and Violence theme picks up a variety of discriminatory terms, whilst the “Acronyms” theme will pick up attempts to hide discriminatory language |
| Drugs / Substance abuse | -displays or promotes the illegal use of drugs or substances. | | This is covered entirely by the “Drugs and Addiction” theme |
| Extremism | -promotes terrorism and terrorist ideologies, violence or intolerance. | | As previously described, this is covered by a PREVENT specific theme along with overlap from other areas |
| Pornography | -displays sexual acts or explicit images | | The “Pornographic Content” theme is designed to pick up thisactivity. Smoothwall suggest this is augmented by high quality web filtering. |
| Self-Harm | -promotes or displays deliberate self-harm. | | The “Suicide and Health” theme will pick up suicidal ideation, and self harm |
| Suicide | -suggests the user is considering suicide. | | The “Suicide and Health” theme will pick up suicidal ideation, and self harm |
| Violence | -displays or promotes the use of physical force intended to hurt or kill. | | Violence will be picked up by the “Racism and Violence” theme |

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

RADAR's themes are constantly being revised. Since becoming part of the Smoothwall family, RADAR benefits from Smoothwall's Digital Safety Analysis team. Over the coming months, we can expect to see new themes, as well as improvements to existing work. Theme content is rated from 1-5 to ensure the highest priority incidents can be alerted as soon as possible.

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

RADAR is generally not used in a blocking context. In order to avoid over-alerting, a number of suppression rules are used to prevent inadvertently tripping the analysis engine. Alerts are combined in the RADAR portal such that it is easy for administrators to sort false positives.

## 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. This will in turn define which alerts are prioritised and responded to | | RADAR can be customised by user or machine group, and alert accordingly |
| • Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided | | Alerts in RADAR are managed by the School. For a managed safeguarding service, Smoothwall suggest the Visigo product. |
| • BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (i.e. not owned by the school), how this is deployed and supported and how data is managed. Does it monitor beyond the school hours and location | | BYOD monitoring is not advised with RADAR client software – students' own devices are not often well secured enough to prevent removal, or properly identify the user. Smoothwall suggest using web filtering to monitor unmanaged devices. |
| • Data retention –what data is stored, where and for how long | | Data is stored in a UK based Microsoft Azure data centre. Data retention is for 1 year |
| • Devices – if software is required to be installed on devices, the monitoring system should be clear | | A software install is required. Windows, macOS, Chromebook |

| | | |
|---|---|---|
| about the devices (and operating systems) it covers | | and iOS are supported. |
| • Flexibility – schools ability to amend (add or remove) keywords easily | | Schools are able to exclude keywords |
| • Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard | | RADAR is available as a multi-tenant solution on request. |
| • Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools? | | RADAR is capable of displaying an AUP to students. In addition, Smoothwall offers guidance around best practice. |
| • Multiple language support – the ability for the system to manage relevant languages? | | RADAR currently supports English and Arabic, this range will be expanded during 2019 |
| • 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? | | Alerts are prioritised based on their severity – grading is a combination of RADAR's inbuilt grades, and School input grading |
| • Reporting – how alerts are recorded within the system? | | Alerts are recorded within the RADAR portal. A full reporting suite is available as well as a real-time dashboard. |

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

| |
|---|
| RADAR is specifically designed to be easy-to-use and intuitive. This ensures that the software can be used by the entire staff in order to ensure that the school's online safeguarding responsibility is fulfilled.<br>RADAR's Pre-Grading feature automatically assigns a level of risk to each instance of captured activity radically reducing the amount of time spent on assessing activity and ensuring that instances of risk are easily identified.<br>Automatic reporting, alerts and a highly-visual user interface ensure that staff can instantaneously<br>identify potential incidents of risk allowing early intervention and escalation where necessary. An upgrade path to Smoothwall Visigo offers a managed safeguarding alert service for schools with changing requirements. |

Shaw Education Trust

We believe, you achieve


Shaw Education Trust Head Office,
Kidsgrove Secondary School,
Gloucester Road,
Kidsgrove,
ST7 4DL

Twitter: @ShawEduTrust
LinkedIn: @ShawEducationTrust
Tel: 01782 742910
Email: info@shaw-education.org.uk
Online: www.shaw-education.org.uk