smoothwall

The Web You Want

Keeping Children Safe in Education

A Smoothwall Perspective

Issued

June 2016

In May 2016, the Department for Education released its revised statutory safeguarding guidance for schools and colleges, 'Keeping children safe in education', replacing 'Keeping children safe in education' July 2015.

The document issued under section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Non-Maintained Special Schools (England) Regulations 2015, outlines that schools and colleges must have regard to 'Keeping Children Safe in Education' when carrying out their duties to safeguard and promote the welfare of children.

It should be read alongside statutory guidance 'Working together to safeguard children' and departmental advice 'What to do if you are worried a child is being abused - Advice for practitioners'.

This revised guidance will commence as of 5th September 2016 and should be read and followed by all governing bodies of maintained schools and proprietors of independent schools, who will need to ensure that ALL staff in their school read at least part one of the guidance.

The Department for Education states that it is essential for children to be safeguarded from potentially harmful and inappropriate online material, such as abuse, substance misuse, bullying and radicalisation. Governing bodies and proprietors must therefore now not only ensure they have the most appropriate 'web filtering' in place but also the appropriate 'monitoring' in place.

The aim of this document is to demystify the facts around online safety and take a closer look at how Smoothwall can help schools with regard to appropriate filtering and appropriate monitoring, which is featured heavily as part of the new legislation.

Online Safety: Why now?

The increasing use of technology within schools has meant that it has become a notable component of many safeguarding issues, including but not limited to **child sexual exploitation, radicalisation and cyber bullying.**

Unfortunately, whilst technology in schools can greatly improve academic learning, it has also become a platform that facilitates harm. It is therefore essential that you have an effective approach to online safety to enable you to empower your school or college, whilst protecting your community in their use of technology. It also gives you the power to establish ways to identify, intervene and escalate any incident where appropriate.

What are the three main areas of risk?

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm

From September 2016 all governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school or colleges IT system and as part of this process you should ensure your school has appropriate filters and monitoring systems in place.

Filtering

What is appropriate filtering?

Appropriate Filtering takes into account the restriction of access to online material which can be divided into two different categories: Illegal Online Content and Inappropriate Online Content. The Department for Education have outlined the following criteria that must be met in order for your filtering to be deemed appropriate.

Illegal Online Content

When it comes to choosing your filtering provider you should ensure that access to illegal content is blocked, specifically that the filtering providers:

- Are Internet Watch Foundation (IWF) members and block access to Illegal Child Abuse Images and Content (CAIC)
- Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

Smoothwall are a member of the Internet Watch Foundation and implement the CAIC list of domains and URLs. Smoothwall also use a number of search terms and phrases provided by the IWF and their members. We perform daily self-certification tests to ensure that the IWF content is always blocked through a Smoothwall.

Smoothwall also implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

Inappropriate Online Content

A web filtering provider should be able to demonstrate that they can filter and block against content in the following categories. Whilst the below does not provide the full extensive list, it provides an indication towards the capabilities and expectations of the web filter.

- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.
- Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances
- Extremism: promotes terrorism and terrorist ideologies, violence or intolerance
- Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- Pornography: displays sexual acts or explicit images
- Piracy and copyright theft: includes illegal provision of copyrighted material
- Self Harm: promotes or displays deliberate self harm (including suicide and eating disorders)
- Violence: Displays or promotes the use of physical force intended to hurt or kill

Smoothwall provides filtering and reporting for over 100 categories, including **all** those listed above. Smoothwall uses a wide variety of techniques in order to identify and categorise content. All categories use a static list of both URLs and domains, with the majority of categories also using search terms, weighted phrases and regular expressions to identify content on the fly, which forms part of our real-time content aware web filter. Therefore, the underlying categorisation focusses very little on the URLs and instead is mostly based on the content of the page. This weighting mechanism allows sites to be more accurately classified and filtered upon, without unduly restricting access.

Because of the way our system works, we are confident we prevent against overblocking, and ultimately the policies are set by the system administrators, giving them the freedom to block or allow categories or individual pages, and policies can be set to allow access to certain categories to different user groups.

Key Filtering System Features

In addition to the above filtering considerations, the guidance also suggests that your filtering solution should meet the following principles:

- Age appropriate, differentiated filtering: includes the ability to vary filtering strength appropriate to age and role
- Control: has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content
- Filtering Policy: the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking
- Identification: the filtering system should have the ability to identify users
- Mobile and App content: isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies
- Multiple language support: the ability for the system to manage relevant languages
- Network level: filtering should be applied at 'network level' ie, not reliant on any software on user devices
- Reporting mechanism: the ability to report inappropriate content for access or blocking
- Reports: the system offers clear historical information on the websites visited by your users

Smoothwall has the functionality to support all the outlined principles.

Age appropriate, differentiated filtering: Through integration into various directory services, the system administrator is able to apply filtering rules based on the user group.

Control: Our easy to use dashboard and policy management gives the system administrator confidence to manage the filter themselves, and we provide a range of shortcut features designed to simplify making simple configuration changes.

Filtering policy: Smoothwall provides published guides which are currently being re-written to reflect the most recent updates within the product (as of June 2016).

Identification: This is done via our integration with various directory services, so long as the system applies the relevant criteria necessary for identification. Furthermore, we offer a number of different mechansims to ensure users are identified, such as a log-on page, Kerberos, a Chrome plug-in, and others.

Mobile and App Content: Both for local and remote filtering we are able to filter all http and https connections from a client, this is not limited to browser traffic and includes mobile and app connections.

Multiple language support: Smoothwall performs dynamic content analysis in a variety of languages in order to identify content and to ensure schools can monitor or block content in foreign languages as required.

Network level: While remote filtering can be done with or without client software, normal filtering occurs without any software being installed on the clients.

Reporting mechanism: Smoothwall provide a mechanism to report back on inappropriate content for access or blocking.

Reports: The system offers very comprehensive controls over how much data is retained over a time period, and is then made available through a large and powerful reporting tool.

Monitoring

Appropriate monitoring and what is expected

Monitoring can be defined as the activity of supervising or reviewing the activities undertaken by an individual or group, and in this case applies to the specific monitoring of online activity with regards to safeguarding issues.

The UK Safer Internet Centre have defined several approaches you can use to form your monitoring strategy, which should be selected based upon your own risk assessment and circumstances.

Physical Monitoring

This is when your circumstances suggest that your school or college is low risk, and staff in these circumstances will directly supervise children whilst using technology.

Internet and Web Access

This depends upon the web filtering solution providing logfile information that details and attributes websites access and search term usage against individuals. Through regular monitoring, this information could enable schools to identify and intervene with issues concerning access or searches.

Smoothwall collects all online activity records per individual user. Suspicious web searches, blocked activity, bandwidth usage, IP address aduit trail, user audit trail, time spent browsing, top search terms and web searches can all be reported upon within the Smoothwall monitoring system. This gives a complete overview of the online events happening within the school by each user, including students and staff.

Active and Proactive Technology monitoring services

Where the risk is assessed as higher, active or pro-active monitoring technologies may be suitable. These specialist services provide technology based monitoring systems that actively monitor use through keywords and indicators across devices. These can prove particularly effective in drawing attention to concerning behaviours, communications or access.

Active Monitoring: Where a system generates alerts for the school to act upon.

Smoothwall offers a specialist suite of safeguarding tools, which analyses the online activity outlined above and categorises it into one of seven rulesets; radicalisation, suicide, abuse, substance abuse, bullying, criminal activity and adult content. These are then ranked by a scoring system in terms of the level of risk, and fit into one of three groups: caution, warning or danger. These reports are designed to show the intent of the online activity ie. is an inappropriate search term a one off occurence or is it grouped with other actions showing a pattern of behaviour. This tool generates alerts and reports which can be provided to the safeguarding officer to take appropriate action, and can be viewed as **active monitoring.**

Pro-active monitoring: Where alerts are managed by a third party provider and may offer support with intervention.

With regards to **Proactive Monitoring,** which should be considered for high-risk situations, Smoothwall works with a third party solution provider called **e-Safe Systems**, who provide advanced endpoint monitoring for schools. e-Safe is installed on all school owned devices and can monitor keystrokes both online and offline against an advanced threat library. When an alert is triggered, a screenshot of the activity is taken and the alert is then analysed by forensic experts to establish it's credibility. Once this process is complete the school/college will be alerted of the incident. e-Safe provides a truly multi-lingual service and can monitor in all languages and colloquialisms.

Both of the above solutions can montior against the following content, as outlined by the Department of Education: Illegal content, Bullying, Child Sexual Exploitation, Discrimination, Drugs, Substance Abuse, Extremism, Pornography, Self-Harm, Violence and Suicide. You should consider self-assessing the level of risk posed by these issues and consider which type of monitoring solution is most appropriate for you - it is very common to evaluate that you would need both solutions.

Schools should consider how their system integrates with their existing policies, and should satisfy themselves that their monitoring strategy meets the following principles:

- Age appropriate: includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to.
- BYOD (Bring Your Own Device): if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), ensure it is deployed in accordance with policy
- Data retention: should be clear what data is stored, where and for how long
- Flexibility: changes in keywords (addition or subtraction) can be done easily according to an

agreed policy.

- Impact: How do monitoring results inform your policy and practice?
- Monitoring Policy: How are all users made aware that their online access is being monitored? How are expectations of appropriate use communicated and agreed? Does the technology provider, offer any advice or guidance?
- Multiple language support: the ability for the system to manage relevant languages
- Prioritisation: How alerts generated via monitoring are prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?
- Reporting: How alerts are recorded, communicated and escalated?

Smoothwall has the functionality to support all the outlined principles.

Age appropriate: So long as the directory service used makes distinctions between age, then you are able to set rules and alerts based on the configured groups.

BYOD: BYOD monitoring is possible as long as the device is connected to the network, and would be monitored the same way as web traffic. This would include monitoring on mobile apps.

Data retention: Data retention is fully customisable for both period and storage dependent on your preferences and which monitoring solution you are using (Smoothwall or e-Safe). Incident records are retained securely for up to 7 years by e-Safe in line with the Data Protection Act.

Flexibility: Schools can amend or update keywords as needed.

Mobile and App Content: Both for local and remote filtering we are able to filter all http and https connections from a client, this is not limited to browser traffic and includes mobile and app connections.

Monitoring Policy: When the online activity is monitored by Smoothwall, any blocked activity would show a Smoothwall blockpage. We recommend all schools make users aware of the monitoring policy, especially when installing the e-Safe client on devices.

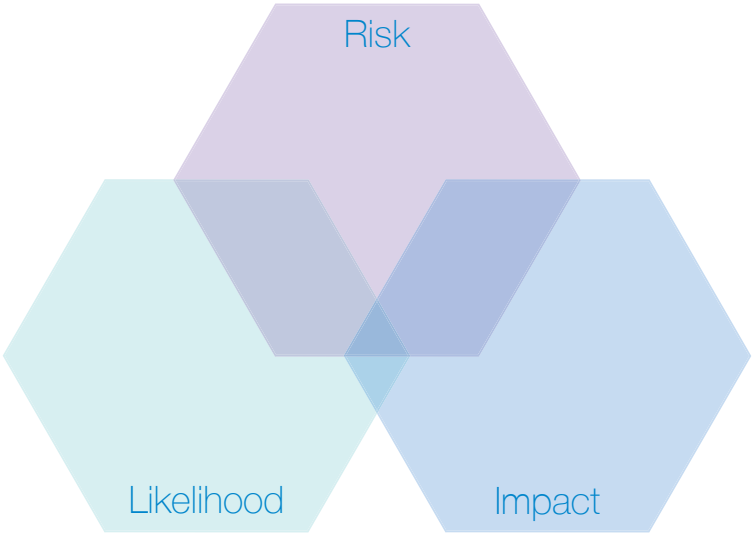
Multiple language support: Smoothwall provides dynamic content analysis in a variety of languages, and e-Safe is able to monitor in all languages.

Prioritisation: Smoothwall rank issues from Caution to Danger based on the activity. e-Safe's specialists are able to individually prioritise the most high risk cases.

Reporting: Dependent on your solution and preferences, reporting can be handled in the best way for your monitoring policy and escalation path.

Choosing the right monitoring solution

To evaluate the right solution you must first assess the risk. A standard model which can be used is to assess the likelihood of an event and the impact of an event and those ranked the highest would be considered high risk.



Those considered low-medium risk will most likely find that filtering and monitoring via Smoothwall will suffice, along with physical monitoring and having a pro-active online safety policy in the school, to protect your risk level. Those considered high risk should consider implementing a proactive monitoring service such as e-Safe Systems, for the extra level of support it provides to you and your users.

How Smoothwall can help

Smoothwall are committed to keeping children safe online and our portfolio is constantly updated to reflect new legislation changes or requirements. Working with Smoothwall we can provide you a complete end-to-end solution, from our established filtering solution used by over 7000 UK schools through to our proactive endpoint monitoring via our third party solutions provider, e-Safe.

For more information about our leading online safety solution, please contact the team or visit our website.

With credit to:

Department for Education

UK Safer Internet Centre
www.saferinternet.org.uk

eSAFE EDUCATION

www.smoothwall.com
08701 999 500
enquiries@smoothwall.com

We're proud of our British heritage.
Our UK Headquarters are based at:

Smoothwall
Avalon House
1 Savannah Way
Leeds Valley Park
Leeds
LS10 1AB
Yorkshire, UK

smoothwall
The Web You Want