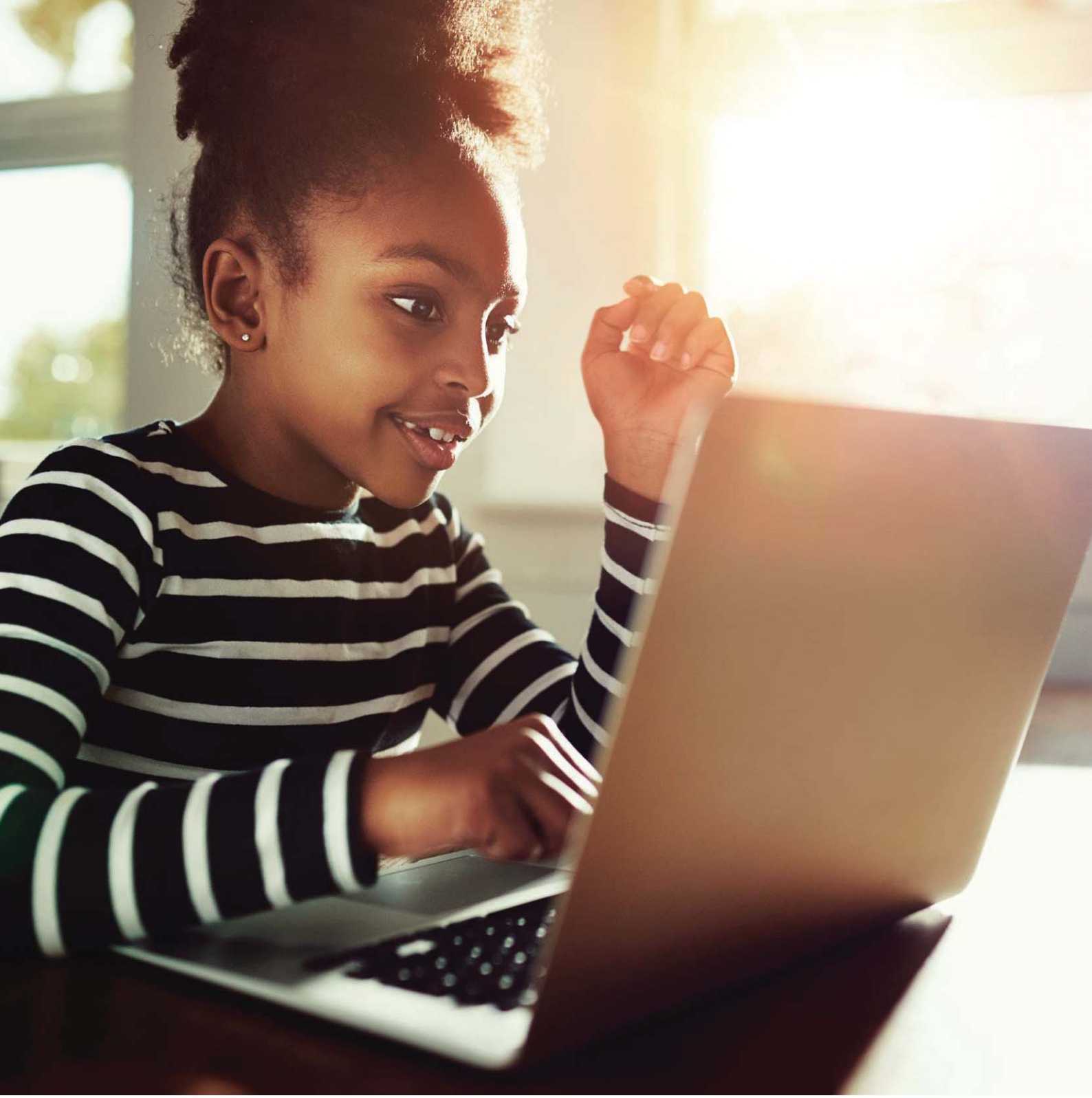


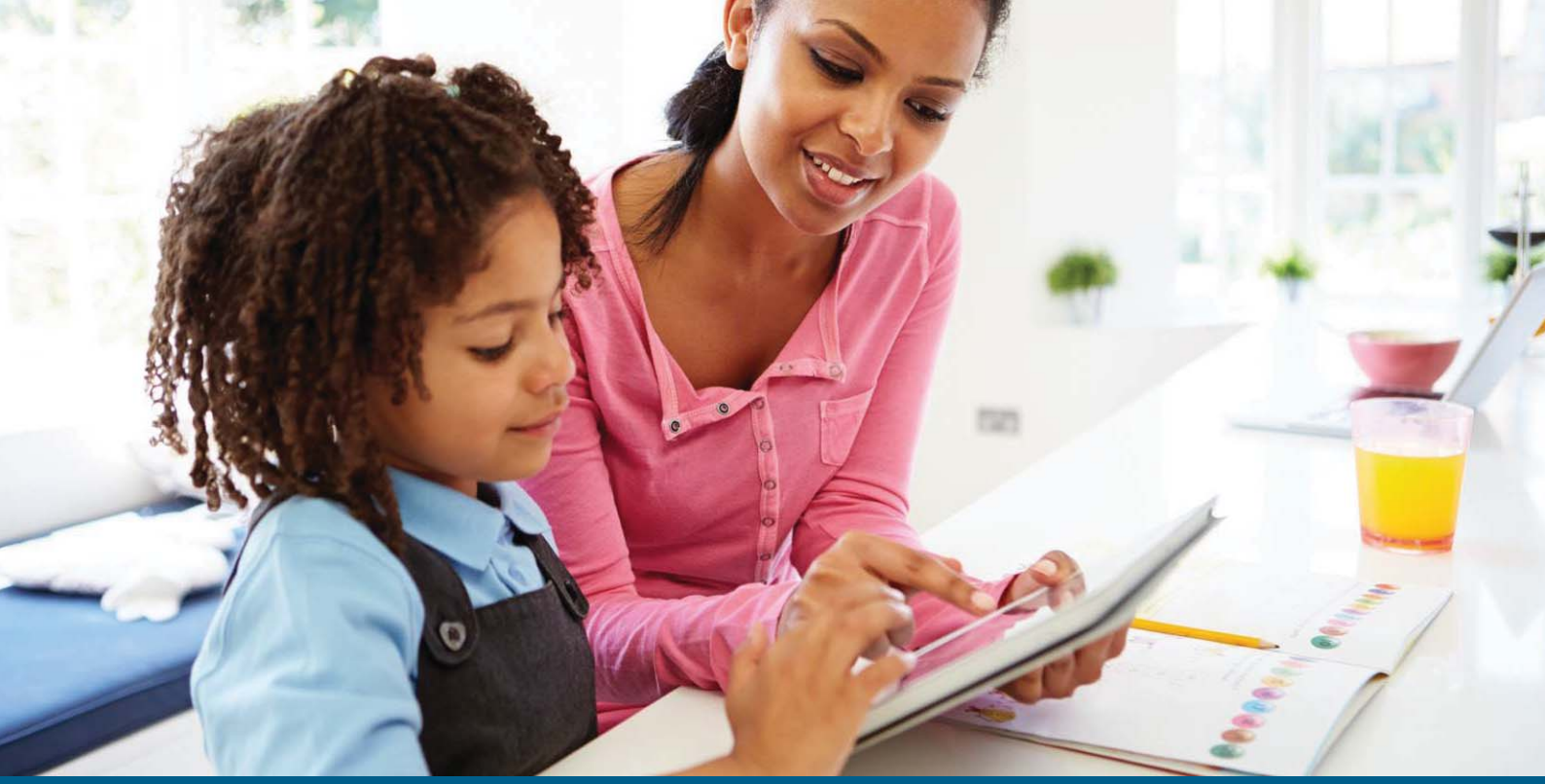
BLUEProfile

YOUR IT PARTNER, Trusted Secure Solutions

Appropriate Web Filtering and Monitoring for Schools and Colleges

SEPTEMBER 2016

SONICWALL™



The new Keeping Children Safe in Education (KCSIE) statutory guidance means that online safety is a critical safeguarding issue.

KCSIE Guidance

Safeguarding is not a new issue for schools but the demands of keeping children and young people safe have grown significantly over the last 10 years. It used to be that abuse was traditionally focused on children in vulnerable groups but the growth in the use of the internet and widespread access to social media mean that all children are now vulnerable to inappropriate and illegal online content.

This has led to the Department of Education (DfE) to update the Keeping Children Safe in Education (KCSIE) guidance, which has been in place since 2014, and an updated version will become statutory on September 5th, 2016. This means that every school will need to consider and review its safeguarding policies and procedures, focusing particularly on how they protect students online.

Department for Education

The Prevent Duty

Following several high profile incidents, the question has been raised as to whether young people are being radicalised whilst accessing the internet in their School or college.

The Counter-Terrorism and Security Act 2015 set out Guidance for specified authorities in England and Wales on their duty to prevent people from being drawn into terrorism. The 'Prevent Duty' is a key aspect of the new KCSIE Guidance and states that "Schools and colleges must ensure that children are safe from terrorist and extremist material when accessing the internet."

Harmful and Illegal Content

The updated guidance mandates that Schools & Colleges employ "appropriate" web filtering and monitoring, in order to safeguard children and young people from accessing harmful illegal content.

Appropriate Filtering & Monitoring

Web or content filtering and monitoring are technical components of online safeguarding and need to be used in conjunction with an overall policy for each individual school, which is well understood by staff and students alike and is reviewed regularly.

Content filtering will provide enforcement of the online policy and monitoring can be particularly effective in drawing attention to concerning behaviours, communications or access.

Conversely, concerning content filtering, the KCSIE guidance warns of the risk of over-blocking leading to "unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

An appropriate filtering and monitoring strategy should ensure that access to illegal content is blocked, specifically that the solution includes the following cornerstones:

- Illegal child abuse images and content (CAIC) using the Internet Watch Foundation (IWF) URL list
- Incorporates 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

Appropriate filtering should control access to inappropriate and harmful content as defined above. In addition, it should be flexible enough to meet the individual needs of each School or College setting a risk assessment.

Ofsted standards and inspection

Since the changes to KCSIE all HMI (Her Majesty's Inspectorate) have received updated training on all aspects of online safety in order to ensure that Schools and Colleges can now meet the requirements of the statutory guidance. Therefore, future inspections are likely to apply much more focus to this area than in previous years and the outcome will directly affect the final judgement.

Harmful content would include areas such as:

Content	Description
Discrimination	promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.
Pornography	displays sexual acts or explicit images
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

Illegal content would include areas such as:

Content	Description
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances
Extremism & Radicalisation	promotes terrorism and terrorist ideologies, violence or intolerance
Child abuse image content (CAIC)	displays specifically images of child sexual abuse including pornography
Piracy and copyright theft	includes illegal provision of copyrighted material

SonicWall Web filtering and Monitoring Solution

SONICWALL™

The SonicWall and FastVue solution is designed to exceed the baseline requirements of KCSIE. By providing integrated web filtering, application control, SSL inspection and anti-malware along with extensive reporting and monitoring, we are able to offer exceptional security and performance to any education setting.

Built around SonicWALL Next Generation Firewalls and FastVue reporting software, we are able to provide a complete, powerful and easy to use solution using class-leading technology.

SonicWall has developed fully integrated security appliances delivering everything you need to protect your network for over 20 years. All SonicWall security appliances feature deep packet inspection firewalls, which act as the first line of defence against security breaches. Integrated SSL/IPSec virtual private networking (VPN) delivers a secure and affordable means of connecting remote locations or staff working from home.

All SonicWall Next Generation Firewalls provide the same level of security and offer the same suite of security services. This ensures we can size the solution to fit both technical requirements and budget constraints. From the smallest pre-school to the largest academy or college we have a solution that fits.

Flexible, affordable content filtering

SonicWall content filtering solutions (CFS) offer the most affordable way to protect your students from harmful and inappropriate web content. CFS is ideal for schools and colleges looking for a cost-effective, integrated solution. Running on all SonicWall network security appliances, CFS features a continuously updated, comprehensive database of over 4 million web sites, domains and IP addresses. With the inclusion of both IWF CAIC and the Home Office terrorism lists, you can be confident students and staff will be protected from the worst content on the Internet.

CFS provides a comprehensive list of 50+ website categories, including all those appropriate to KCSIE such as radicalisation/extremism, drugs, pornography, hate/violence and illegal activities.

Flexible policy design allows for age appropriate filtering and granular control without over (or under) blocking. Integration with Active Directory (AD) means appropriate filtering policies can be applied based on user and user group, enabling individual users to be identified through their AD/LDAP credentials.

Advanced features such as password override mean a teacher can bypass a blocked site for a given period thus avoiding disruption during a teaching session. Policies can then be updated, for example inclusion in a custom allowed list for permanent exceptions.

Other features include custom categories, custom allowed/blocked lists, bandwidth management based upon website category, multiple customisable block pages and confirmation page (logged acceptance before accessing a particular site). See examples in figures 1 and 2.

Blocked website "Splash" screen messages can be customised in order to refer students/staff back to the online safety acceptable use policy, creating awareness along with enforcement (see figure 1).

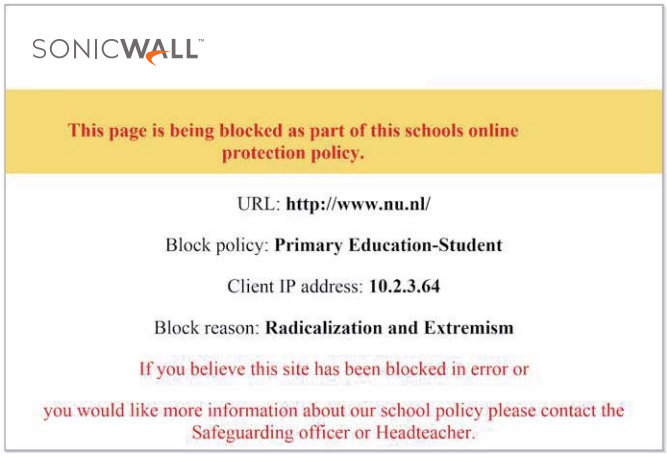


Figure 1 - Block page "splash" screen for 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' list.

Note: the example target domain is purely for demonstration purposes and is neither unlawful nor illegal.

Client content enforcement

Educational establishments can seize control over the Web sites students can access using their IT-issued computers even when roaming and accessing the internet from outside the firewall perimeter. The Content Filtering Client addresses safety, security and productivity concerns by extending the controls to block harmful and unproductive Web content. Supported platforms include Windows, Mac and Chromebooks.

Manage Encrypted Content

Harmful and Illegal web content often lurks deep within social media sites such as Twitter, Facebook and YouTube. Some Schools will simply not allow social media applications to run, however YouTube for example is a Google owned company and has some excellent resources for learning, therefore often the filtering policy will need to be flexible.

Many websites (including Google) are now utilising SSL encryption (HTTPS) as standard, to safeguard personal information when accessing them. Current research shows approximately 25-40% of all web traffic to be SSL encrypted and without the ability to inspect this traffic, your solution is effectively blind.

More concerning, is that without inspecting deep inside the content of encrypted streams, filtering policies will fail to correctly identify harmful and illegal content embedded within trusted social media sites and access may not be blocked.

SonicWall Deep Packet Inspection for SSL (DPI-SSL) allows its users to safely inspect encrypted traffic. Once decrypted, all security services such as CFS and anti-virus can be applied, as per normal unencrypted connections.

Flexible controls ensure "trusted" sites such hosted applications can remain uninspected to ensure maximum performance.

Applying complete visibility and control to application usage

SonicWall gives you complete application visibility and control over which applications are being used on the network, by whom, the bandwidth they are using and what priority they have over your network's valuable bandwidth.

Integrated services

To include additional layers of protection in your network, simply add one or more security services, such as anti-virus, anti-spyware and intrusion prevention, application control or advanced threat protection (ATP/sandboxing). These services run seamlessly on your SonicWall security appliance under a unified management system. And with everything coming from one source, you won't run afoul of complications that pop up when multiple solutions from different vendors don't work well together. It all adds up to lower total cost of ownership.

FastVue Reporting and Monitoring for SonicWall

FastVue provides the ease of use, visibility and monitoring necessary to achieve compliance with the new KCSIE guidance by ensuring policies are being correctly applied and to alert on potential infringements. As a software solution, it provides for flexible deployments across physical or virtual environments.

Designed to work specifically with SonicWall network appliances, FastVue have spent many years developing a simple to use reporting and monitoring solution that delivers clear and concise information, that is easy to interpret for ICT, non-ICT staff and Inspectors alike.

Combining a real-time view of exactly what Internet activity is taking place and historical data, we deliver a reporting and monitoring solution with the ability to alert, block and report, on users searching for illegal or inappropriate web content. Additionally, the system offers clear historical information on the websites visited by your users

Having reporting intelligence easily accessible allows for any education setting to quickly establish it is meeting all legal obligations and its own risk-assessed policies are being applied appropriately. Configurable alerting allows for instant notification of policy infringement or notification for specific activities which may be undesirable.

Below are a number of screenshots showing the types of reports and alerts that are available. This is by no means a comprehensive list, but simply there to highlight some of the capabilities.

Figures 2 and 3 below, show custom reports for sites being accessed that are on 'the police assessed list of unlawful terrorist content, produced on behalf of the Home office' list.

fastvue | Reporter for SonicWall

Figure 2

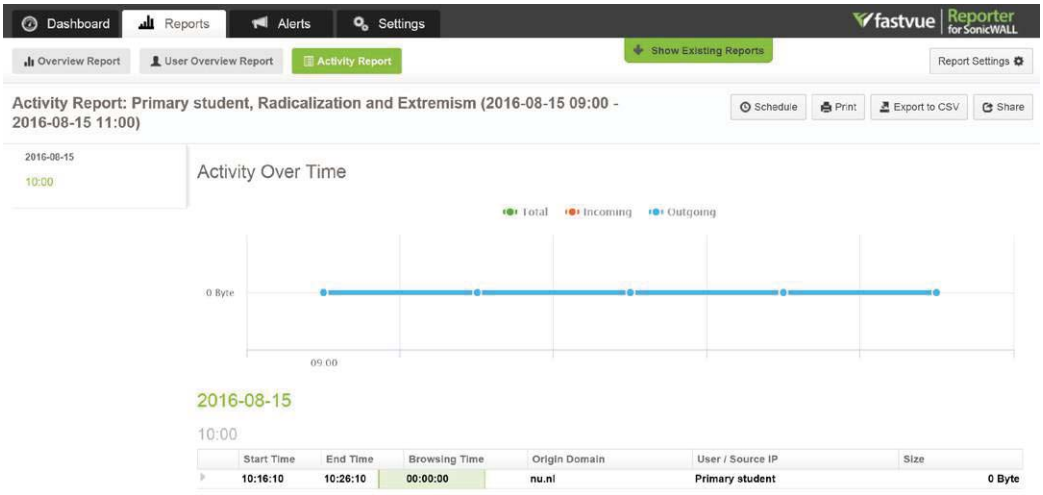


Figure 3

Figure 4 shows a custom email alert when a user "Primary Student" attempts to access a site on the banned Home Office list.

Figure 4

Finally, Figure 5 shows a custom email alert when a user "Primary student" search for specific terms via sites such as Google, Bing or Yahoo which an education setting may deem to be undesirable or potentially be putting a student at risk.

Figure 5

Summary

Each and every school and college in England will need to comply with the new KCSIE statutory guidance and as a result fresh expectation is placed upon those responsible for safeguarding, who, with no additional financial support from Government, will now need to demonstrate much more rigour around online safety policy in order to keep children safe and to pass future inspections. Decisions also need to made around what level of web filtering and monitoring is "appropriate" for each educational setting. This will depend upon a number of factors including the assessment of risk, budget and ICT expertise. The SonicWall/Fastvue solution detailed above places flexibility and control back into the hands of those responsible for online safeguarding. It is granular enough to enforce and inform without hindering learning and delivers reports and alerts to designated safeguarding leads (DSL's) to facilitate decision making, according to policy or passed to inspectors who will want to understand how illegal and harmful content is blocked to internet users.

This results in a key cornerstone of the online safeguarding policy being delivered that provides compliance with KCSIE (depending upon needs/ risk) and most importantly a safe online learning environment for children and young people.

BLUEProfile
YOUR IT PARTNER, Trusted Secure Solutions

DELIVERING TRUE BUSINESS BENEFITS

BLUE Profile's breadth of IT Services and Solutions are designed to add value to organisations and save money & time by identifying and implementing solutions to enhance business performance and increase efficiency & agility

- Managed Services
- Infrastructure
- Cloud
- Network Security
- Professional Services
- IT Support Services
- End User Computing
- Applications & Database
- Backup & Recovery
- Telephony

Proven reliable and backed by our tried and trusted DDIM™ process – we are perfectly positioned to offer you unrivalled levels of expertise and advice.

- DISCOVER
- DESIGN
- IMPLEMENT
- MANAGE

SONICWALL okta ORACLE simplivity SOPHOS EGNYTE

Lenovo vmware CITRIX DELL Microsoft Hewlett Packard Enterprise

Braemar Court, 1311D Melton Road, Syston, Leicester, LE7 2EN
sales@blueprofile.co.uk
0116 218 2120