Appropriate Filtering for Education settings

June 2021

Filtering Integrator 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*" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's 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."

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 integrators illustrate to education settings (including Early years, schools and FE) which filtering solution they utilise/recommend and what additional services they provide that enhance the filtering system to support schools. 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	Superfast Schools
Address	Trevenson House, Church Road, Redruth, Cornwall, TR15 3PT
Contact details	hello@superfastschools.co.uk
Date of submission	27th September 2021
Filtering System Used/Recommended	Combination of WatchGuard / DNSWatch / Senso.Cloud

Please indicate why this filtering system has been adopted or recommended

We operate a tiered approach to content filtering, ensuring that the solution is flexible, secure and does not negatively impact teaching and learning with overly-intrusive rules. All URL categories are updated multiple times a day, both by the vendor using lists provided to them by ForcePoint (a leading provider in Web Filtering) and also by our parent company iCT4 team members as CiSP partners (Cybersecurity Information Sharing Partnership) operated by the UK NCSC (National Cyber Security Centre).

Our filtering system is aware who the user is and the type of user they are – different rules can be applied so that filtering is appropriate and tailored to the user and what they must access in order to be able to deliver the curriculum and learn effectively. As filtering is user-aware it can be configured to be appropriate to age and user type. Filtering is applied at the Gateway and designed to circumvent the use of VPN and/or proxy servers and ensures that all devices connected to the school LAN are filtered, regardless of whether they are owned and managed by the school or not. Optionally, device can be filtered using an agent present on their device (which can feed into our monitoring solution) and additionally supports filtering away from the network, in cases such as remote and/or hybrid learning.

Our WatchGuard hardware is delivered 'as-a-service' allowing us to offer schools unparalleled security of their networks against cyber threats such as ransomware, zero-day threats, phishing and other web-based exploits. Whilst many providers focus on content filtering, supplying a basic firewall, we approach this as a holistic system that requires best-of-breed technology at every step to secure our schools, their users and their data.

On request schools are trained to allow them to manage the filtering themselves, but all staff have access to our helpdesk to raise un-filtering requests as appropriate. During onboarding the filtering requirements are configured with a key contact at the school (e.g. DSL/SLT) and any changes that could materially affect the security of the system are authorised by them prior to implementation.

MAT-level visibility over reporting is available via our 'Reporter' system, offering a dashboard for central oversight. Filtering policies can also be applied at MAT level where centralised control is desired.

If relevant, please indicate how you enhance the filtering system

As an additional safeguarding measure, we have partnered a leading provider of safeguarding solutions to offer Superfast Schools 'Ultimate' customers access to their safeguarding software. This is available for Windows/Chromebook/iPad and supports monitoring of web activity as well as keystroke logging and AI-driven image detection. It is a flexible, secure and reliable solution for home or hybrid learning where devices are away from the school network.

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

At Superfast Schools we work with our users to upskill them, including training for on-site teams such as IT Technicians and/or 3rd parties, IT Coordinators (Curricular) and opportunities for Online Safety briefings via our parent company iCT4 limited.

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

INTEGRATOR 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	Glyn Pascoe
Position	Managing Director
Date	27th September 2021
Signature