

White Paper

WaveConnect Cloud vs On-Premise Web Filtering & Firewall Solutions in UK Schools

Introduction

The education sector is undergoing a significant shift towards cloud-based IT infrastructure. While migrating certain applications and services to the cloud offers clear benefits, it is not always the right choice for every aspect of school IT. Just because a service can be moved to the cloud does not necessarily mean it should be.

UK schools share common operational needs, security requirements, and financial constraints. While their IT requirements may resemble those of enterprises, factors such as government funding models, safeguarding responsibilities, and distinct educational objectives introduce unique challenges. Years of underinvestment, lack of strategic planning, and the influence of local and national policies have further complicated schools' ability to modernize IT effectively.

Many schools and multi-academy trusts (MATs) view cloud services as a solution to these challenges.



WaveConnect Cloud vs On-Premise Web Filtering & Firewall Solutions in UK Schools



Introduction cont'd

Cloud adoption reduces the need to purchase, maintain, patch, and upgrade on-premise hardware equipment that quickly becomes obsolete and requires skilled IT support.

Financially, hiring and retaining IT staff is expensive, and unexpected hardware failures or software upgrades pose significant budget risks.

Outsourcing some IT functions—particularly for widely used services available "off the shelf" can be a pragmatic choice. Large cloud providers such as Amazon Web Services (AWS) and Microsoft Azure have invested billions in cloud infrastructure, while software vendors have transitioned critical applications such as finance, enterprise resource planning (ERP), and productivity suites (e.g., Xero, Sage, Salesforce, Office 365) to the cloud. These services offer cost savings, scalability, security, and accessibility.

However, cloud adoption in education becomes more complex when dealing with services that are highly specialized, such as **web filtering and firewall protection**.

This paper explores the **advantages and disadvantages of cloud vs. on-premise solutions** for web filtering and firewall protection. It considers cost, security, compliance, reliability, and long-term sustainability to provide schools and MATs with a framework for making informed decisions.

Many UK cloud-based filtering providers do not operate on AWS or Azure but instead rely on proprietary infrastructure. These sector-specific platforms often **lack the scale, resilience, and engineering expertise** of global cloud providers, raising concerns about performance, reliability, and security. Furthermore, UK schools are advised to implement **dual internet links** for resilience. However, most cloud filtering providers route both internet connections into their **centralized infrastructure**, meaning that if their core platform experiences issues, both links are affected. In contrast, an **on-premise solution** can leverage dual internet connections from **separate ISPs and technologies** (e.g., leased line + FTTP), ensuring direct, independent access to the internet without reliance on the same data center platform. Additionally, **on-premise firewalls and web filters can be configured with automatic failover appliances** at minimal cost, providing a **highly resilient and cost-effective** alternative.

1. The Regulatory & Security Landscape in UK Schools

Schools in the UK operate under strict safeguarding and cybersecurity obligations. Web filtering and firewall solutions must comply with:

- **Keeping Children Safe in Education (KCSIE)** – Ensuring students are protected from harmful online content.
- **The Prevent Duty** – Schools must prevent access to extremist materials and radicalisation content.
- **UK GDPR & Data Protection Act** – Ensuring secure handling and processing of student and staff data.
- **Department for Education (DfE) and National Cyber Security Centre (NCSC) Guidance** – Outlining best practices for school cybersecurity.

Failure to meet these requirements can have serious **legal, reputational, and financial consequences** for schools and Trusts. A **secure, resilient, and well-managed filtering and firewall solution** is essential.

2. The Case for Cloud-Based Web Filtering & Firewalls

Potential Benefits:

- **No On-Site Hardware Requirements:** Schools do not need to install or maintain physical appliances.
- **Scalability:** Cloud services can easily expand for additional sites or capacity.
- **Managed Security Updates:** Regular patches and security enhancements.
- **Expert support:** Qualified engineers to maintain and support the platform

Challenges & Risks:

- **Performance & Latency Issues:** Cloud-based filtering and firewall traffic often route over multiple clusters/proxies introducing contention and latency. Customers should request detailed information about contention and routing.

WaveConnect Cloud vs On-Premise Web Filtering & Firewall Solutions in UK Schools



Challenges & Risks cont'd

- **Limited Customisation & Control:** Schools often have minimal control over filtering policies and firewall rules as wider access is a risk to the service providers other customers on the same platform. Customers should satisfy themselves that they have the required management access and responsive support.
- **Mismatched functionality:** Many of these self-constructed multi-tenanted platforms are built on solutions that were not designed to support hundreds of tenants/domains.
- **Data Security & Compliance Concerns:** Third-party storage of sensitive student data introduces GDPR risks. Customers should evaluate providers data security arrangements.
- **Limited Resilience & Expertise:** Unlike AWS or Azure, many UK education-sector cloud filtering providers operate on sub-scale infrastructure, lacking global-scale engineering and security resources. Customers should satisfy themselves that suppliers have appropriate skilled resources and contingency in the event of absence or unplanned resource issues.
- **Dependency on Centralised Cloud Infrastructure:** Even if a service provider deploys dual internet links, both connections are often routed through the same application cluster (Web-filtering/Firewall/DNS) negating much of the benefit of a backup connection.

3. The Case for On-Premise Web Filtering & Firewalls

Traditional on-premise solutions have historically faced concerns such as:

- **High upfront costs** for hardware and software.
- **Ongoing maintenance requirements.**
- **The need for technical expertise** to manage the infrastructure.
- **Scalability challenges** when expanding to multiple sites.

4. WaveConnect : A Modern Approach: Co-Managed On-Premise Web Filtering & Firewall Solutions

A **co-managed on-premise solution** eliminates the traditional concerns while retaining **the security, control, and reliability benefits** of local infrastructure.

How a Co-Managed On-Premise Solution Addresses These Challenges:

The Solution	
✓	No Upfront Costs – WaveConnect is charged annually. Schools avoid large capital expenses, making the service cost-effective.
✓	Pro-active Patching and Updates - Always up to date, secure
✓	Hardware Upgrades & Replacements – Hardware is replaced as needed, with no concerns about aging equipment.
✓	Unlimited Helpdesk Support & Changes – Schools receive unlimited troubleshooting and modifications.
✓	Direct Control & Customisation – IT staff retain full access to firewall and filtering rule management, but the provider ensures continuity if key staff leave or there's a skills gap.
✓	Dedicated Infrastructure per School/Trust – No shared resources, ensuring better performance, security and performance.
✓	True Dual Internet Resilience – Schools can use two independent ISP connections with diverse technologies , ensuring continuous service even if one provider experiences issues. Both connections can be load-balanced, offering additional capacity.
✓	Low-Cost Automatic Failover – Schools can implement an automatic failover appliance for enhanced reliability at a minimal additional cost.
✓	Advanced Security Benefits – On-premise firewalls inspect local data traffic (peer-to-peer, peer-to-server, unmanaged devices, BYOD) for cyber threats, malware, and ransomware activity - something cloud firewalls cannot do without routing all traffic through the cloud , increasing latency and bandwidth use.
✓	Core Outages Impact Individual Schools Only – Unlike cloud solutions where a core failure affects all schools in a MAT , an on-premise failure impacts only the individual school.

Conclusion

- Cloud-based filtering solutions offer convenience but have security, control, and resilience limitations.
- Traditional on-premise solutions had drawbacks, but modern co-managed on-premise services eliminate concerns.
- As IT evolves, Schools and Trusts need maximum flexibility and support to meet challenges.