Visit rm.com

RM™

Insights

The future of learning, powered by RM Technology

Autumn 2025
Issue 01

4 steps to a successful digital upgrade

One trust's story of boosting their cyber security

Your quick guide to the KCSIE updates

P.19 Win an RM x Zen hoodie!

Beyond block lists

TOOLS AND TIPS > BEST PRACTICE > PRACTICAL SOLUTIONS > STRATEGY

Welcome to RM Insights

What's inside?

We're building trusted partnerships for education

"Welcome to the first issue of our new customer magazine. Having recently taken up the post of RM Technology CEO, I'm honoured to launch this magazine, which we hope will become an invaluable tool for leaders across the education sector.

My journey, through developing curriculum and classroom resources as CEO of another of RM's divisions, TTS, has shown me how transformative the right technology can be. This understanding truly shapes our approach to supporting schools and trusts with the tools they really need.

This first issue focuses on keeping schools safe—a responsibility we all share. Today's educational landscape presents unprecedented challenges. Cyber threats evolve daily, requiring robust security that doesn't compromise teaching and learning; online safeguarding demands vigilance as learners navigate digital spaces and schools are exploring AI's potential while managing its risks; all within increasingly stretched budgets.

For multi-academy trusts, these challenges multiply across sites. As your trusted partner, we understand that technology isn't just about installing kit. Instead, it's about creating secure, sustainable environments where education thrives. Whether managing cloud migration, improving broadband and network connectivity, or providing responsive support, success depends on understanding each trust's unique context.

Inside you'll find insights, best practice and practical solutions drawn from our experience as a comprehensive technology partner. We hope this will help you in addressing the real challenges you face and offer actionable guidance.

Get in touch and let us know what you think of this first issue. You can email me at lmackinnon@rm.com."

Ian Mackinnon,
CEO, RM Technology

Come and meet the team at this term's events and webinars. Details at rm.com/events ›

Beyond the block list: balancing protection with educational access

The DfE's filtering and monitoring standards require an effective filtering system to block internet access to harmful sites and content. At the same time, it should allow legitimate teaching and learning activities and not make school administration unnecessarily difficult.

Effective content filtering really depends on understanding age-appropriate content and the needs of individual learners, as well as a filtering system that makes it easy to manage differing requirements.

With mainstream schools increasingly handling diverse needs, and special schools embracing technology to support learning, age or year group might not match emotional or social developmental needs, making flexible and responsive systems a must.

Danielle Doman, the designated safeguarding lead for a school that serves secondary-age learners with needs related to 'communication and interaction' and 'cognition and learning' told us how they handle the challenge of protecting their learners when online.

Beyond age bands: understanding individual filtering needs

Each year group will have learners at different developmental stages, academically and emotionally. Applying age-based filtering settings should be seen as a starting point. There will typically be individual learners who don't fit a neat age-based category for filtering or monitoring.

This is when systems with user-based filtering come into their own. Having identified learners with particular needs, the ability to edit default settings and apply them to a single user, or a group of users with similar needs, protects them in a personalised way.

Examples of circumstances when standard age-based filtering can be unsuitable:

- fixations
- developmental differences
- obsessive behaviours.

In these cases, school leaders should make decisions about filtering and monitoring based on the individual vulnerabilities of the learner. Settings can change according to the subjects and topics on the curriculum at any given time.

> **"We don't work to age-related expectations at our school. So even though a child may be in year 11, it doesn't mean we'll give them access to what a typical year 11 child would be able to have access to, based on their academic ability and their emotional ability."**
>
> **Danielle Doman,**
> Designated Safeguarding Lead,
> Sutton School, Dudley.

Meeting the challenges of obsessive or fixated behaviour

Certain types of SEND can be associated with obsessive or fixated behaviours, presenting a potential danger for learners when online. The desire to discover more and more about a particular topic can result in exposure to inappropriate content types. This intensely pursued interest can also result a learner neglecting other areas of their study.

User-based filtering can help proactively support learners who display obsessive or fixated behaviour by restricting access to content on specific topics. The ability to quickly adjust settings prevents escalation of problematic behaviours. Adaptable filtering systems give teachers the confidence that their learners can research topics independently, without being taken into unsuitable areas or spending too much time on them. Being able to tailor settings before a class studies a particular topic also provides reassurance for parents that their child will be safe when online in school.

Teacher's perspective:

"Our pupils can become fixated on certain elements and we need to steer them away from those problems. Some of them aren't aware of the risks that they may be incurring."

Creating flexible filtering frameworks

Meeting safeguarding obligations, such as Keeping Children Safe in Education (KCSiE) and the DfE's filtering and monitoring standards, requires multiple layers for different users. The framework for effective filtering has four levels:

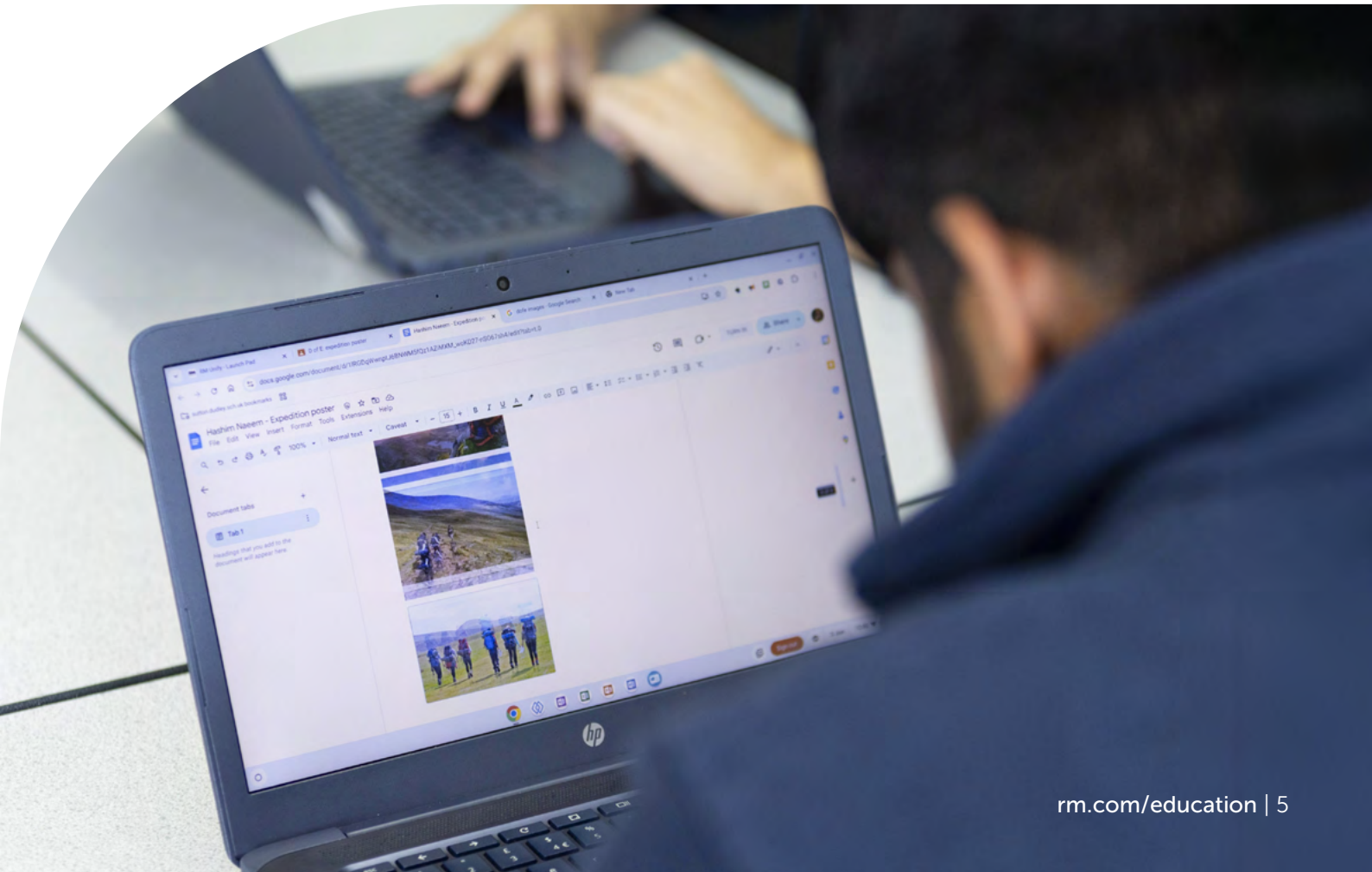
- Default year group settings
- Class-specific adjustments for curriculum topics
- Individual learner restrictions or permissions
- Staff access levels

Most attention is rightly given to ensuring that learners only access appropriate online content. However, staff needs shouldn't be overlooked. Staff may have additional access needs to be able to provide for their class. They also need to be free of the worry that learners might access inappropriate content in class. By basing the filtering arrangements on the four levels mentioned above, schools can have the right level of flexibility, balanced by robust safeguarding for all.

Recognising the requirement to manage individual user or group settings according to need can become a burden rather than a benefit if the filtering system doesn't allow those responsible to make changes quickly and easily.

DSL's perspective:

"Our staff definitely feel more confident knowing that our pupils are safe. They know that our pupils can use their own independence to research what they need to but they won't be taken down a path to things they're not allowed to. Staff also have that additional option to have more access for what they need to be able to provide for their class."



Collaborative approach to filtering decisions

Effective filtering requires partnership between a school's IT support, teaching staff and senior leaders responsible for safeguarding.

As with all safeguarding matters, staff need to know how to raise concerns and when to take the appropriate action. IT support should maintain filtering and monitoring systems, make changes according to agreed processes, and provide senior leaders with filtering and monitoring reports.

Having a defined process for curriculum-based requests to increase access or needs-based requests to restrict it is critical to managing the needs of individual learners or groups. The DSL can judge the desirability of the request, and the school's IT support will implement the decision.

"Staff will come to me and our IT manager to ask for things to be changed or to amend certain things."

Danielle Doman,
Designated Safeguarding Lead,
Sutton School, Dudley.

Safeguarding staff can use reports to check whether any pupil's access requirements should be reviewed and communicate changes to teachers.

DSL's perspective:

"Based on the reporting system, we're also able to see which of our pupils could possibly be looking for the wrong thing. It may be for individual pupils, we feel that they're not allowed to be looking at a certain area, and we know that it needs to be removed."

Recommendations for implementing effective filtering

Filtering systems must block access to the types of risk outlined in KCSIE – harmful content, contact, conduct and commerce. Schools should also use the risk assessment required by the Prevent Duty to inform their filtering and monitoring choices.

Filtering and monitoring systems must incorporate lists of illegal websites provided by The Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU), at a minimum.

Schools should implement flexible filtering arrangements that accommodate individual needs resulting from SEND or other factors and can be adjusted according to circumstances. This flexibility and the ability to make changes quickly enable good teaching and protect learner wellbeing.

Your quick guide to the Keeping Children Safe in Education (KCSIE) updates

By Tasha Henstock,
RM SafetyNet Product Manager

The DfE published the 2025-2026 academic year version of Keeping Children Safe in Education (KCSIE) on 1st September. Although there are no substantial changes, this version is now in force. School and trust leaders must ensure that their settings follow this statutory guidance:

Main updates

Part 1: Safeguarding information for all staff

Part 1 is unchanged. All staff working directly with children should read part 1 of KCSIE as a minimum. Staff not working directly with children can read the condensed version found in Annex A.

Part 2: The management of safeguarding

New content risks

The list of safeguarding harms now includes three new types of content risk. They are misinformation, disinformation (including fake news) and conspiracy theories.

Definitions

KCSIE does not give definitions for these types of content, so here are helpful explanations:

- Misinformation is false or out of context information that is presented as fact, regardless of an intent to deceive.
- Disinformation is a type of misinformation that is intentionally false and intended to deceive or mislead.
- Conspiracy theories are the belief that certain events or situations are secretly manipulated behind the scenes by powerful forces with negative intent.

Actions

- Adjust relevant policies to reflect the new wording.
- Ensure filtering and monitoring systems handle these types of content.

Part 3: Safer recruitment

Links to gov.uk services to use when conducting background checks are given.

Generative AI

The section providing guidance on suitable filtering and monitoring arrangements now includes a link to the DfE guidance on safety expectations for AI products. Although mainly meant for product developers and suppliers, the guidance forms a convenient checklist for schools when evaluating the use of these products.

Actions

- Review the DfE standards on filtering and monitoring, particularly how filtering and monitoring requirements apply to generative AI.

Alternative provision

A school's responsibilities when placing a pupil with an AP provider now include obtaining information about staffing at the AP, keeping records of the location(s) and undertaking regular reviews of attendance and suitability.

Attendance

The section on absence from education now requires schools to work with local authority children's services where school absence suggests safeguarding concerns.

What's next?

Each edition of KCSIE aims to improve safeguarding for children. Although not in the latest version, to inform your future thinking, future iterations are likely to include links to updated guidance on Relationships, Sex, and Health Education and revised guidance on gender questioning children, plus reflect the progress into legislation of the Children's Wellbeing and Schools Bill alongside ongoing government audits, inquiries and strategy work.

To find out how RM can help bolster digital safeguarding in your school or trust,

get in touch – rm.com/contact >

New cyber security features for RM Broadband

National Cyber Security Centre's Protective Domain Name System

Last year, the NCSC announced that its PDNS for Schools service would be available to various types of schools and school internet service providers (ISPs). PDNS is a security system designed to help keep you safe when browsing the internet. It blocks access to known malicious or suspicious online destinations, such as websites known to host malware, ransomware, viruses, and other cyber security threats.

Rather than requiring schools to take action themselves and request the service via their DNS provider or ISP, RM worked with NCSC to implement PDNS across our entire estate. It's included for RM broadband customers at no additional cost for schools of all types, not just those mentioned in the NCSC announcement.

One of our largest broadband customers is HFL Education. HFL's Broadband Lead, Kevin Crawley, appreciates RM Broadband's commitment to making customers more cyber secure:

"Providing NCSC PDNS for schools across the network has improved cyber security for HFL Broadband's customers without them needing to lift a finger or divert budget from other areas."

Kevin Crawley,
Broadband lead, HFL Education.

Police CyberAlarm for your first line of defence

Police CyberAlarm (PCA) is a free and secure cyber threat tool funded by the Home Office and delivered by the police. It monitors suspicious activity targeting external systems such as firewalls and antivirus solutions, functioning similarly to an external CCTV for digital infrastructure.

Top tip

Installing the PCA provides monthly threat and vulnerability reports that detail indicators of compromise, intrusion attempts, high-risk vulnerabilities, and emerging attack patterns. These reports enable schools to patch outdated software, investigate suspicious logins, and update firewall rules, ultimately strengthening overall cyber hygiene and security posture.

Again, RM has implemented PCA at the network level. Once the school is registered with PCA, RM can switch it on for RM Broadband customers upon request. This removes the need for schools to deploy additional infrastructure or install, configure, and deploy it themselves.

"We are proud to be working with RM to make cyber security simpler and more accessible for the education sector. I recently led a training session for the RM team and was impressed by their commitment to and enthusiasm for improving cyber security for schools."

Andy Richmond,
National Co-ordinator, Police CyberAlarm.

2025 FINALIST ISPA AWARDS BEST CUSTOMER, NETWORK AND DATA SECURITY www.ispa.org.uk/ispa-awards

These cyber security innovations contributed to RM being shortlisted in the Best Customer Network and Data Security category in the ISPA Awards 2025.

The 'Safety and security' section of our blog has posts on NCSC PDNS and Police CyberAlarm - scan the QR code for more.

Plan, invest and grow your technology

The four-step path to successful digital upgrades

Upgrading the technology provision in your school or trust needs careful planning to maximise your investment. We've identified four elements that will deliver successfully on the promise of new technology in the classroom.

These steps will help you reimagine your classroom with dependable, education-ready technology delivered with RM's wraparound support.

01 Step one - build the foundation

Devices

Start strongly with reliable, education-ready devices that support day-to-day teaching and learning. This phase focuses on robust, secure, and performance-driven hardware built for the classroom.

Devices need to withstand the rigours of classroom use. Carefully chosen devices with up-to-date components and operating systems will deliver day-after-day, year-after-year, and have the lifespan to confidently justify your investment.

Top tip

One size doesn't necessarily fit all. Your school will likely need a blend of device types, with Chromebook, desktop, and laptop options to meet the needs of different users. Mobile and desktop workstations are necessary as pupils take on more specialised work.

Infrastructure

It's essential to consider whether your existing infrastructure can support the demands of connections from new or more devices. Your investment priorities might change as a result.

> **"Our vision was about devices and connectivity, and infrastructure. Other schools talk about having amazing devices, but without the connectivity, it's futile."**
>
> **Paul Stimpson**,
> Assistant Head Teacher and ICT Coordinator,
> Kirkby Woodhouse School, Nottinghamshire.

Why does infrastructure matter in phase one?

- Cloud-based tools rely on strong connectivity
- Devices need dependable WiFi and power
- Interactive displays require secure network access
- Desktop labs and admin systems all depend on robust back-end systems

02 Step two - enhance every lesson

Displays

Interactive display technology enriches lessons by boosting classroom interaction between teaching staff and the pupils or among learners.

Teaching staff can control front-of-class displays from anywhere in the classroom, allowing them to interact with pupils around the classroom.

Learners can collaborate and share work from their devices by casting content or resources from a device to the big screen, or vice versa, with support for different operating systems.

What to consider in this phase?

- Could you enhance existing technology platforms, such as Google for Education or M365, using interactive displays?
- Possibilities for integration with teachers' devices to streamline lesson preparation and delivery
- Can screens be managed centrally to improve energy efficiency, simplify app deployment and support school-wide communication?
- Stand and mount options can support flexible use

Ready to start your journey? Email getintouch@rm.com >

03 Step three - **connect and collaborate**

More devices, with increased capabilities, demand greater management and setup resources. Both users and the devices themselves need to be integrated into school and trust systems to ensure effective security and safeguarding.

When choosing management tools aim to:

- Make it easy to access learning apps and cloud platforms via single sign-on
- Provide individuals and groups with appropriate access rights using data taken from the MIS, backed up with an audit trail
- Reduce password resets and avoid repetitive admin work for IT staff.
- Get lessons underway quickly with speedy access to resources
- Standardise and streamline device setup and management.

04 Step four – **sustain and grow**

From trade-in schemes to lifecycle support, this phase ensures your hardware stays reliable and cost-effective while giving you a platform for what's next.

Stretching your budget, sustainably

Manufacturer trade-in schemes help your budget go further when replacing or adding to your school's devices. Careful planning of renewal schedules will reduce the outlay needed to update and replace laptops, desktops or Chromebooks.

Top tip

Trade-in also simplifies disposing of old devices with collection, data erasure and responsible recycling or repurposing

Ready to start your journey? Email getintouch@rm.com

Boosting cyber security - one trust's story

RM has worked with a multi-academy trust of approximately 30 primary schools to assess and improve its cyber security arrangements using Cyber Essentials as a benchmark. For the purpose of this article, we've not named the trust in order to protect it from the attention of cyber criminals.

The challenge:

The trust has embarked on a digital transformation programme involving the standardisation of its operating model for its central functions, and the trust's IT team needed to address cyber security.

Everyone wanted to reduce the likelihood of a cyber attack disrupting their central operations. The trust's culture avoids a high level of prescription from the centre, which must be balanced against an appropriate level of cyber security provision.

The IT team decided on Cyber Essentials as a benchmark for their central operation's cyber security position. The trust understood that it was unlikely to meet the scheme's requirements. Without the internal resources to identify where it would fall short and how to close the inevitable gaps, it engaged RM's Cyber Essentials Consultancy service to help.

The solution:

One of RM's cyber security experts worked with the trust to create a holistic view of its Cyber Essentials readiness. The client received a comprehensive report with recommended steps to take. The process also delivered a toolkit to help the trust achieve compliance.

The project ran to an agreed schedule to maintain focus and prioritisation. In this case, it took roughly eight weeks, including the Christmas break.

> **"We're becoming incrementally safer by following the road map that we developed with the RM consultant."**
>
> Trust Programme Director.

Steps in the project:

1. Self-assessment to establish a baseline for tracking progress.
2. A gap analysis by the consultant.
3. An action plan provided by the consultant and agreed with trust stakeholders.
4. Regular meetings between the consultant and the trust to review progress and provide direction and support (during this period, the trust completed some of the identified actions using resources provided by RM).
5. Consultant delivered the final report with a list of completed actions plus those still outstanding, ranked according to their respective importance.

The outcome:

- The trust now understands its cyber security risks more fully.
- Using RM tools, the trust has eliminated some existing vulnerabilities found during the process.
- The project report provided the trust with a list of topics to address, with defined actions and owners. RM provided tools, including policy templates and process guidance, to help complete these actions.
- Having spoken to the RM consultant during the project, the trust's senior leadership team now understands that cyber security is an ongoing process.
- The scope of the consultancy project was to determine how likely the trust's central operations were to comply with Cyber Essentials. However, additional vulnerabilities emerged, and the final report listed them and provided suggestions for addressing them.
- As the trust implements the report's recommendations, it improves its cyber security position and reduces its overall risk.

> **"It felt very driven by our needs. It felt very personal, but it also felt that we were getting a significant level of expertise."**
>
> Trust Programme Director.

Looking to improve cyber security at your school or trust? Get in touch for a free consultation on how RM can help – rm.com/contact

RM Technology Awards

The inaugural RM Technology Awards recognised outstanding achievements among our school and MAT community, showcasing success stories in innovation, safety, and operational excellence.

Six categories of excellence

School Trust of the Year

Celebrated MATs demonstrating forward-thinking, trust-wide technology strategies implemented from the top down.

Engineer of the Year

Recognised technical achievement over the 30 years of RM being an Internet Service Provider (ISP).

The Keeping Schools Safe

Highlighted exemplary use of technology and policy for physical and digital student safety, including cyber security and safeguarding best practices.

The Digital Champion

Highlighted exemplary use of technology and policy for physical and digital student safety, including cyber security and safeguarding best practices.

Primary School of the Year and Secondary School of the Year

Recognised schools using technology to create exceptional learning outcomes and deliver operational excellence.

Awards at prestigious event

RM Technology's executive leadership team and sponsoring partners served as judges, assessing the entries according to pre-agreed criteria. The winners were announced at a ceremony during the pre-dinner drinks reception at the CST Annual Conference on 16th October.

Congratulations to all nominees who received recognition graphics and goodie bags, while winners took home trophies and the opportunity to be featured in professional case studies showcasing their achievements.

The awards showed how schools and trusts are using technology to transform education delivery and learner outcomes.

Check our LinkedIn feed to find out more about the winners and nominees.

In profile:
A look at the people behind the technology

Simon combines technical expertise with a genuine understanding of schools' needs. His innovations haven't just got schools connected, they've shaped how millions of pupils safely access digital learning.

Matt Bearpark,
Head of Product, RM.

Simon Rainey's three-decade journey of innovation in educational connectivity

Simon Rainey is one of RM's internet consultants, working in the broadband development team. As RM celebrates its 30th year as an internet service provider (ISP), we asked him to reflect on the innovations and developments he's seen in his nearly 30 years with RM.

When Simon joined RM, the internet was a digital free-for-all. Schools faced a choice. They could embrace digital technology with its attendant risks or remain disconnected from the online educational revolution. Simon identified a third path. He would make the internet safe for schools.

The birth of content filtering

In 1996, few people had grasped that schools needed protection from inappropriate online content. Rather than wait for someone else to solve this problem, Simon built the solution himself. Starting with a Netscape proxy server and manually curated block lists, he developed what would become RM SafetyNet—the web filtering system that now protects thousands of UK schools.

Writing custom C code, Simon created a filtering architecture that remains the foundation of today's system. His innovation wasn't just technical; it addressed schools' needs. He understood that schools required a specific type of protection, designing real-time content filtering that could scale across entire education networks.

Bridging the bandwidth gap

Simon's innovations extended beyond safety. Recognising that schools needed higher bandwidth than typical small businesses but lacked the necessary budget, he pioneered a technique called ISDN channel bonding. It delivered 128kbps connections and addressed a fundamental market gap, providing schools with the connectivity they needed at prices they could afford.

Scaling security

The early 2000s brought new challenges, with Regional Broadband Consortia requiring unified security for thousands of schools. Simon designed a central firewall architecture using Checkpoint technology, which later evolved using other platforms. This innovation made enterprise-grade security standard for all RM school connections.

Rather than accepting expensive individual school firewalls, Simon's centralised approach provided appropriate security without impractical costs. Today's system allows individual schools to manage their own firewall policies built on this robust foundation.

Future-focused engineering

One of Simon's strengths is anticipating challenges before they impact customers. When Regional Broadband Consortia began dissolving, he foresaw IP address conflicts as schools switched providers. His Logical Customer Network solution created virtual firewalls, allowing schools to maintain existing IP addressing schemes and avoid costly network renumbering.

Connecting rural communities

Understanding that educational equality requires universal connectivity, Simon tackles the challenge of rural schools through 4G, satellite, and hybrid solutions. His technical assessments of emerging technologies like Starlink demonstrate continued innovation whilst preventing costly implementation mistakes.

Advanced security

Simon stays ahead of evolving threats, implementing the National Cyber Security Centre's PDNS at network level whilst blocking circumvention methods including VPNs, DNS over HTTPS, and other techniques. His proactive approach maintains the protective environment schools require.

Lasting legacy

Most importantly, Simon combines deep technical expertise with a practical understanding of educational needs. He continues to write code and implement solutions personally. Simon hasn't just brought connectivity to UK schools, his work has defined how educational institutions safely access the digital world.

Simon's contribution to schools technology has been recognised in this year's Internet Service Provider Association's Awards. We're proud that Simon is a finalist in the Engineer of the Year category. He will also receive one of the inaugural RM Technology Awards.

Read all about it

Here's what some of our RM colleagues have been up to recently.

September, the busiest month

Support engineers Wil Weaver and Peter Jackson reflect on a job well done at Kemball School, part of The Orchard Trust in Stoke on Trent. RM has been working with the trust to migrate operations to the cloud. Wil and colleagues decommissioned the old servers across the trust, as well as enrolling devices on Microsoft Intune.

Partner training day

Our account management and sales teams' held a two-day 'Back to School" session in late August. It helped deepen their knowledge of how our products and services can help schools in the new academic year.

HP brought their HP van for a hands-on look at the latest hardware for the classroom.

Police CyberAlarm provided an overview of how this new collaboration is keeping RM schools safe and secure.

Other sessions, including those from Google, Trend Micro, ViewSonic, and several broadband partners, completed two days of focused learning. We also celebrated a special milestone: Zen Internet and RM Technology are both celebrating 30 years as an ISP! You can win one of our commemorative hoodies on page 19.

Connected Britain

RM's Matt Bearpark, Adam Day and Mike Butler attended the Connected Britain event which brings together industry experts, innovators, and policymakers to shape the future of the UK's digital economy.

It was a great opportunity to further learn how we can best drive connectivity and the digital landscape across schools and colleges.

Be in it to win it!
Win a hoodie

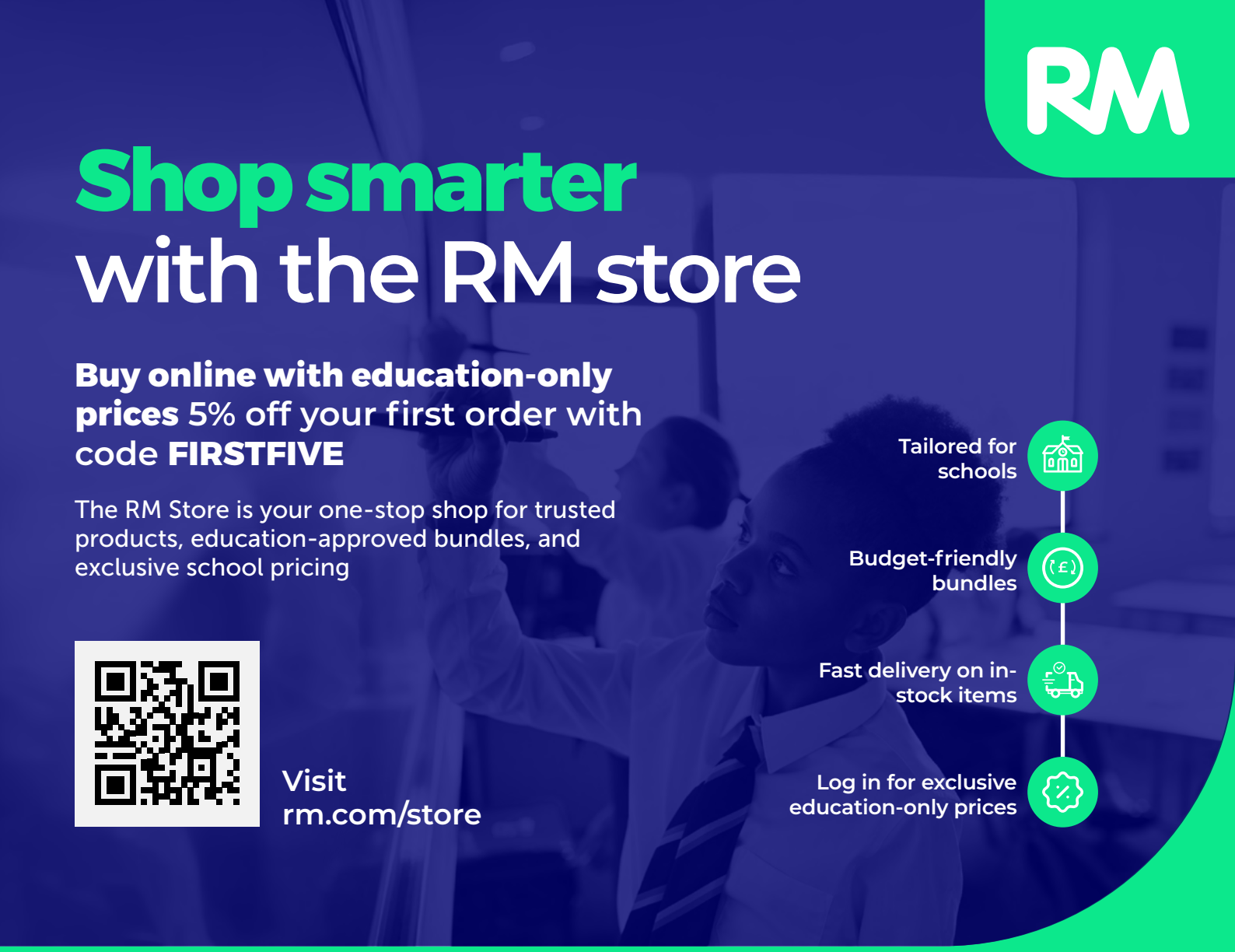
This year, Zen and RM are jointly celebrating our 30th anniversaries as internet service providers. As part of our celebrations, we're offering you the chance to win one of our fabulous commemorative hoodies, as pictured below.

Our models: Zen's Kelly Holt, Channel Account Manager and RM's Head of Product Matt Bearpark and Will Digby, Broadband Product Manager, alongside Mark Titman, Zen's Partner Sales Manager.

To be in with a chance of getting your hands on one of your own, simply subscribe to receive this quarterly magazine and/or our monthly email newsletter TechTalk at www.rm.com/about/newsletter.

We'll pick one lucky subscriber at random on November 31st as our winner.

See our terms and conditions at rm.com/terms.



Shop smarter with the RM store

Buy online with education-only prices 5% off your first order with code **FIRSTFIVE**

The RM Store is your one-stop shop for trusted products, education-approved bundles, and exclusive school pricing

Visit rm.com/store

- Tailored for schools
- Budget-friendly bundles
- Fast delivery on in-stock items
- Log in for exclusive education-only prices

Get in touch

To find out more about how RM can help your school or trust make the most of technology, contact us at rm.com/contact

Register now to make sure you get future issues of RM Insight at rm.com/about/newsletter

Subscribe to our email newsletter at rm.com/about/newsletter

Follow RM Technology on LinkedIn for the latest updates.

Head Office: 142B Park Drive, Milton Park, Milton, Abingdon, Oxon, OX14 4SE T: 01235 645 316