eSafety in schools

Sophie Beyer asks experts from industry and teaching how do we keep kids safe when using the latest edtech?

Q. Whose job is it to keep children safe online? Where do the responsibilities begin and end for the educational institution?

Al Kingsley: Fundamentally it's the role of all adults working in or on behalf of a school who have the responsibility to safeguard and promote the welfare of children. Under the umbrella of *Keeping Children Safe in Education* schools have a responsibility to provide a safe environment in which children can learn, as well as constantly monitoring and identifying any child that may need additional help or be at risk of harm.

Stella James: The truth is it is all our responsibility to protect children both off and online. Many parents view online safety as a problem for schools to solve, leaving some parents totally unaccountable and free to remain blissfully unaware of the threats they and their children face online.

Simon Pridham: The lines of responsibility are blurred, especially if children are bringing their own devices to school, or using the internet at home to do their homework.

Laura Knight: Online safety is best viewed as part of the school's responsibility to safeguard the young people in its care. In a fast-changing digital world, strong connections need to be created between parents and teachers, as old boundaries about what used to be left at the school gate are no longer valid.

Henry Seddon: Parents and teachers need to supervise and monitor the use of the internet. This starts by getting online then understanding and educating oneself about the risks. Once the risks are understood, parents and teachers need to start a conversation about the risks, potential problems children may encounter and rules around internet use.

Mark Bentley: The first part of the question is an easy one – it could not be made clearer in the key DfE document *Keeping Children Safe in Education* that it is everyone's responsibility. Technology allows bullying to continue

Image © freepiks.com

seamlessly beyond the school day and gate. At LGfL we are building a centre of excellence in safeguarding to help schools more.

Q. What risks exist for children online? Which risks can schools most help mitigate?

Al Kingsley: Children are digital natives, where the use of online tools is seen as a natural extension of their communication tools – and the caution and self-checks on potential implications that adults might apply are often absent. From bullying, radicalisation (Prevent duty), to child sexual exploitation, the risks are significant. The two key strands a school can use to help mitigate are: educating children on the risks, and employing effective monitoring tools so that activity can be identified quickly and effectively.

Stella James: Children are sharing and exposing so much personal data and using tools online such as live video streaming with no guidance or effective education. Children are at risk from everyone and anyone online for the purposes of sexual grooming, befriending, exploitation, radicalisation and online bullying and all in the safety of their own home. ➡

EXPERT OPINION:
MAKING SCHOOL ESAFETY PRACTICAL AND EFFECTIVE

By Al Kingsley, Group Managing Director, NetSupport Limited

There are many different eSafety solutions available on the market today, but how do you choose the one that will work best for you?

With many pressures on staff time, whether you are a teacher, safeguarding lead or an IT technician, finding a solution that is efficient, but doesn't create significant extra work is paramount. NetSupport DNA has been designed specifically with schools in mind, so that it instantly delivers the data and notifications you need, but doesn't negatively impact already-busy work schedules.

WHAT TO LOOK FOR

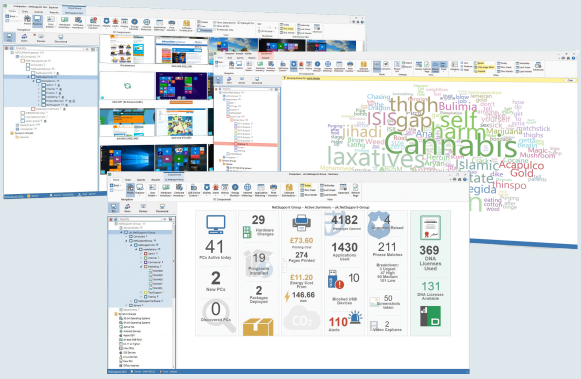
Good solutions will focus on providing alert data in the most accessible format possible to allow staff to see at a glance who the student is, what they're doing, and where the device is located.

Efficient network and IT asset monitoring can track the PCs students use and the applications they are using, while smart keyword and phrase monitoring can alert teachers to any high-priority events as they occur. Further safeguarding measures such as endpoint security (to ensure students can't share inappropriate content at school via USB sticks) and a way for students to share their own concerns with trusted teachers, should also be a consideration.

TIME IS OF THE ESSENCE

The quicker staff can see what is happening via clear, visual on-screen information, the sooner they can take the appropriate action to deal with activities of concern. NetSupport DNA allows staff to see alerts and trends in seconds, meaning that safeguarding is as timely, practical and effective as can be.

Learn more about NetSupport DNA at www.netsupportdna.com/education

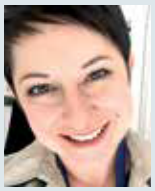


CONTRIBUTORS

AL KINGSLEY
Group Managing Director of NetSupport Limited

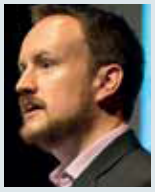
STELLA JAMES
Founder of Gooseberry Planet

SIMON PRIDHAM
Former headteacher, is education director Aspire 2Be.



LAURA KNIGHT
Director of Digital Learning at Berkhamsted School

HENRY SEDDON
VP EMEA at Duo Security



MARK BENTLEY
from London Grid for Learning Safeguarding Board

BEVERLEY SMITH
Director of Friendly WiFi

GRAEME LAWRIE
Director of Innovation at Sevenoaks School

SARAH WILLIAMSON
Director of Information Systems at Sevenoaks School

Main image ©depositphotos.com

Simon Pridham: The risks at home are many and varied, and can include accessing age-inappropriate material such as violent or sexually explicit imagery, engaging in risky or illegal behaviour such as online gambling, or falling victim to fraud, ID theft, blackmail, online grooming, child abuse or religious radicalisation. Schools' IT networks must have filtering and blocking software to stop children accessing harmful content and monitoring systems

Laura Knight: Online risks fall into four categories: contact, conduct, content and commercial. Children may find themselves victims of online predators, may behave in inappropriate ways, they might access adult, extreme or illegal content, or will be subjected to inappropriate advertising or commercial interactions. Schools are required to provide appropriate filtering and monitoring systems as part of Keeping Children Safe In Education, and are required to ensure that children are taught about staying safe online.

Henry Seddon: Despite the highly publicised cases of exploitation involving the internet, for the clear majority of children, for most children, the internet will be a wonderful experience. However, risks range from exposure to inappropriate material, harassment, financial or legal risks, and even exposure to physical risks by children arranging meetings through the internet. Children need to be able to discuss openly what they encounter online and what they like doing online, no matter how trivial, and learn the impact the internet can have.

Mark Bentley: Schools can't take away risks any more than parents can. The key is that we equip young people to face them, and crucially make sure they know where to go to for help, advice and where to report when something goes wrong. Teaching critical thinking in the online arena is very important. The open-access 'Trust Me' resource from LGfL and Childnet is very useful in this respect.

Beverley Smith: Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the risks from the school or college's IT system by ensuring appropriate filters and monitoring systems are in place. There remains no replacement

Many parents view online safety as a problem for schools to solve, leaving some parents blissfully unaware of the threats

for vigilance, realism and good practice, but a Friendly WiFi-approved venue will block access to pornography and web pages known by the Internet Watch Foundation to host indecent images of children. That removes a huge level of risk at source. The danger, however, is a moving target and a 'block list' is updated twice a day.

Sarah Williamson: The balance between protection and education is shared by everyone involved in welfare and teaching at Sevenoaks School. As well as embracing the latest technologies and preparing our students for the digital world they will live and work in, our Technology and IT teaching covers privacy settings, passwords, ransomware, hacking and malware. Our PSHE programme looks at the social impact of issues like grooming, cyberbullying, obsession and addiction, sexting, body image, personal safety and financial security. New risks emerge constantly and schools need to keep up-to-date with changes to statutory requirements such as the government's Prevent strategy aimed at keeping children safe from exploitation and radicalisation.

Q. Are teachers and educators aware of all the risks? Is there enough training and CPD provided for teachers?

Al Kingsley: The risks are constantly evolving. Only last month we had the fresh challenge of so-called 'suicide games' like the Blue Whale game, plus games that risk injury like the Salt and Ice challenge or Neknomination. The key is that training and intelligence sharing need to be a constant and ongoing process within the school. There is a risk with a never-ending focus on standards that insufficient time is spent on a child's broader education and that staff do not have sufficient time for their wider CPD in areas such as this.

Stella James: I think schools only know a fraction of what is happening. We have apps like Music.ly, Roblox and Live.ly. Online Safeguarding cannot simply be a box-ticking exercise. Something as complicated and important as online safeguarding should be ongoing.

Laura Knight: We are all learning, all the time. I think it is important to promote a principles-led approach which does not require every teacher to worry about every feature of every app, but focuses instead on encouraging kindness, empathy, good decision-making and authenticity. We risk missing the boat and not equipping students with the understanding and support they need to process what they encounter until it is too late. (According to the NSPCC, the average age that a child first views pornography in the UK is 11.)

Q. How can schools educate children to behave with respect and consideration online?

Simon Pridham: The purpose of school is to educate children and prepare them for life in the real world. As part of this mission teachers already teach children how to treat others with respect and consideration, reinforcing positive behaviour and reprimanding poor behaviour. There's no reason this approach can't be transferred to their online activities too.

Mark Bentley: It is much easier to be rude to someone online than face to face (think Twitter trolls!), so one challenge worth tackling is teaching young people that if you know how to behave offline, then mirror the same respect and courtesies online. Why not check out some anti-bullying materials at bullying.lgfl.net for example.

Q. What products, resources and technologies exist to help teachers?

Al Kingsley: There is a range of solutions designed for filtering access to online resources at the perimeter of a school network. Increasingly, the most effective solutions are ones that work on a local device level and can monitor safeguarding keywords that may indicate a child is at risk of harm, can capture screen and supporting behaviour information for more serious topics (such as suicide or radicalisation) and help build a picture of trending topics to steer school assemblies. The latest generation of safeguarding and IT management solutions also provide self-service lists of safeguarding resources for children to access – covering everything from FGM helplines to drug and bullying resources.

There is a wealth of forums and online resources available to teachers. Firstly, ensure all staff know their KCSIE obligations ➡

"Governing bodies and proprietors should be doing all they reasonably can to limit children's exposure to risks from the school's or college's IT system"

and then organisations such as the Internet Watch Foundation provide resources for child sexual exploitation; the UK Safer Internet Centre provides resources on eSafety and tools; technical forums like EduGeek provide a great platform to find out about the tools available for use in a school, from schools who already use them; and industry leaders, like NetSupport, will provide on-site discussions with Safeguarding teams on how solutions can be tailored to meet a school's needs.

Stella James: Quality resources are vital. I am going to say Gooseberry Planet. We are the only company that offers 12 weeks of education for each child in each year of their primary education. The NSPCC, Childnet, SWGL, ParentZone all have resources for one-off lesson plans which are very good and there are some great products that are comprehensive and offer consistent learning. E-Cadets is another good example.

Henry Seddon: Parents and teachers should speak to internet service providers and understand if they can limit access to certain places on the internet. The files children download should be monitored and parents may want to consider sharing their children's email addresses. Finally, many browsers can block inappropriate material through parental controls – choose a browser that allows this and enable it through the settings.

Mark Bentley: LGfL has collated resources, advice and guidance from a range of providers into a one-stop portal at osresources.lgfl.net. There are materials for the classroom, for policymakers (such as templates for acceptable use policies) and for parents. And if you need to talk to someone, you can't go wrong with the Professionals Online Safety Helpline – helpline@saferinternet.org.uk.

Beverley Seddon: Friendly WiFi, launched in partnership with the The UK Council for Child Internet Safety (UKCCIS). It is the first – currently the only – such service anywhere in the world.

Sarah Williamson: It can be tricky for schools to find lesson resources and activities that engage students – they are a tough crowd to teach about technologies they use far more than we do! Organisations like CEOP, NSPCC, Childnet, Internet Matters and ParentZone provide excellent toolboxes of information, activities and resources. Sometimes it's useful to team up with other schools to share good practice, external speakers, ideas and resources. Conferences, workshops and training events are invaluable.

Q. Are parents fully aware and what products or resources could help them?

Al Kingsley: Absolutely not. The landscape is ever-changing and the functionality available within applications is constantly changing, often introducing a fresh risk in applications that were previously vetted and deemed safe. All OS providers now provide some form of child protection controls, time limits and activity recording, and schools should encourage parents to review the tools available for each desktop and table

platform. One of the more challenging areas to police, however, is the forum-based chat capabilities within console-based games. These are often the hardest to manage. A simple 'door open' policy when gaming at home can be a great start. Good practice is to also encourage the school IT department to provide regular updates to parents on tools that may support their efforts to keep their children safe online.

Laura Knight: Unfortunately, I do not believe that all parents are aware of the issues and often they are unsure of where to turn to get help. There are some fantastic tools online for parents and teachers, and simply getting involved with what children are doing and asking questions is the best starting point. Networking with other parents and searching for help from recognised organisations such as CEOP and the NSPCC will also help.

Henry Seddon: I would strongly suggest using Chromebooks. They are lightweight, have long battery life and are relatively cheap to buy – plus they come with built-in security through the Chrome OS which has built-in virus and malware protection and is always updated to the latest version – so you never need to worry about malicious files using a Chromebook. In addition, they can be set up in supervisor mode which enables activity monitoring and limiting.

In addition we recommend having controls on the router governing your network that have parental controls enabled to prevent against inappropriate content. Open DNS is a great router filter that can help with this.

Graeme Lawrie: Without being prescriptive to parents about the device their child may use in school, we try to offer advice about the features that work best. Parents are best placed to manage individual contracts with their own ISPs and smartphone providers to make sure access is age-appropriate. Contracts for children should always bundle controls and filters. There are many invaluable resources to direct parents to, including Digital Parenting, which gathers positive advice, information and reference in one publication. Above all, online safety experts urge parents to keep non-judgemental dialogue open with their children, so they can explore any concerns about the use of technology whilst understanding the attractions.

Q. How is it best to discuss online safety with children?

Stella James: We need to allow our children to talk about their experiences. So many schools and adults, just want to block, which is so wrong and not actually that helpful if we want our children to be responsible and independent users of technology. We do not have the attitude of never allowing our children outside because of the dangers, we don't lock them away. We teach, we embrace and we guide. Online safety is no different.

Laura Knight: Little and often! Online safety is not a box that can be ticked just once in an academic year. It should be embedded into lots of contexts so that children can learn to appreciate the different angles. In school, we bring online safety into our curriculum through PSHE and ICT, through whole school termly assemblies, and parent talks. Using peer mentors and digital leaders is also worthwhile to reduce a 'them and us' culture.

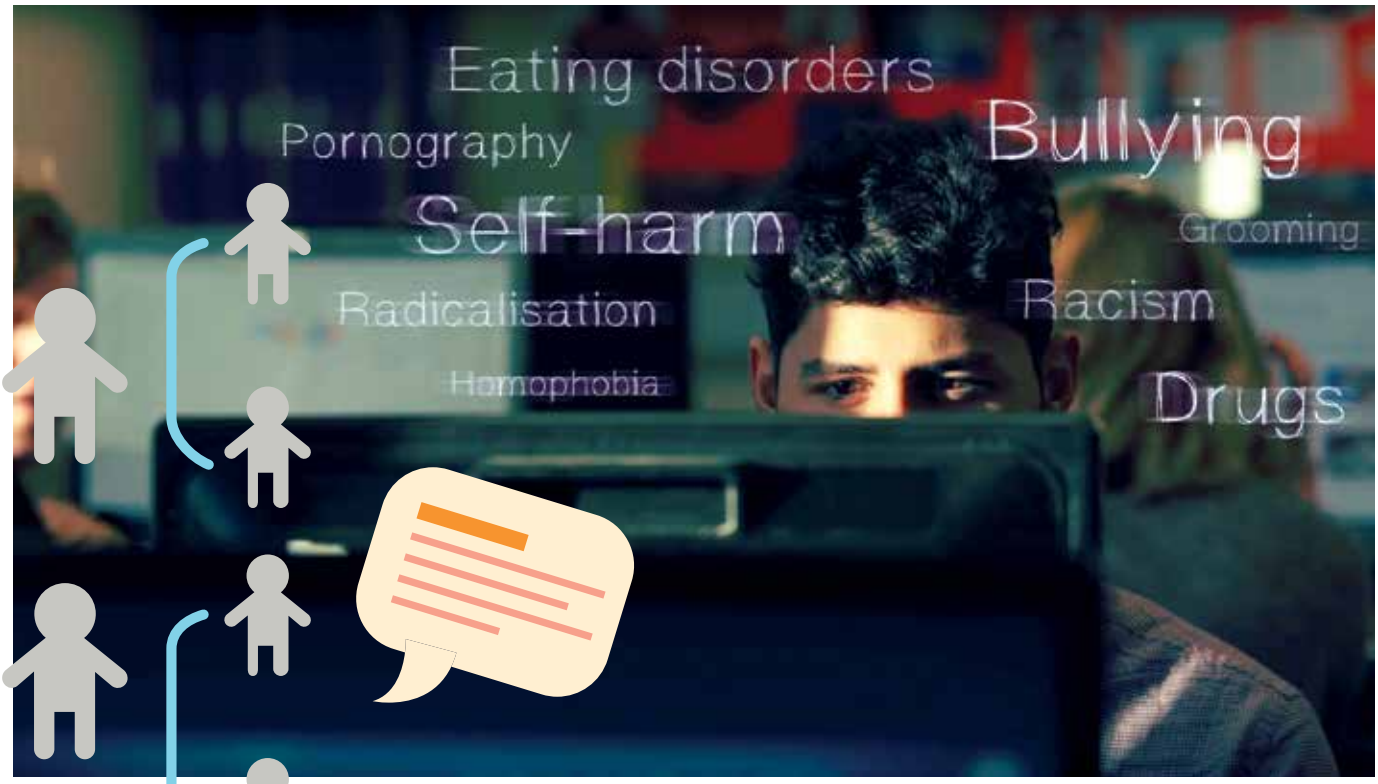
Mark Bentley: All the time! There is no offline and online life anymore, so limiting online safety to a specific time or teacher is not appropriate – it needs to be threaded through all we do.

Q. How can teachers encourage wellbeing and healthy habits?

Stella James: Being open is the biggest key to any child's wellbeing. We are all human, we all make mistakes, it is part of learning.

Simon Pridham: Teachers can encourage healthy online habits by encouraging an open and honest classroom discussion about the issues involved. Rather than frame the issues in negative terms such as 'banned websites' or 'restricted content', teachers should reinforce positive online behaviours and advocate personal responsibility. Pupils have to be trusted to use devices and the internet responsibly, but they have to earn that trust and then repay it.

Mark Bentley: There is a wealth of wellbeing resources available to help on the curriculum side of things; toolkits such as Adolescent Resilience from LGfL and Public Health England give valuable signposting in this area. But an interesting question to ask at the same time is – do teachers model wellbeing and healthy habits ➡



Main image © depositphotos.com

to their pupils? Given the framework in which they work and the average work-life balance of a teacher, this is a tricky one.

Q. Does bring your own device help or hinder online safety?

Al Kingsley: It's a double-edged sword. On one level, having a range of devices and platforms being used within the school network adds an extra layer of management for the school IT department – this often comes with a cost and increases the risk that the normal controls enforced on desktop devices are missed on tablets, for example. However, the silver lining is that, with parental consent, monitoring tools installed on school devices under a BYOD policy can be used to protect the student away from the school as well. As with everything surrounding safeguarding, it's about intelligence and visibility, so that help can be offered no matter what location the child is in.

Simon Pridham: BYOD is a policy that is increasingly being implemented by schools. If schools have a detailed policy to manage BYOD use and systems to ensure compliance then there should be no additional online safety issues to using the school's own devices. Schools should have an IT system that only allows guest devices to join if they comply with the e-safety policy.

Mark Bentley: BYOD is a fact of life, and whilst current usage is patchy (some schools embrace it; some schools ban it), the direction of travel is clear. When considering implementing a BYOD policy schools should consider what the opportunities and challenges are. In an age of austerity for schools, opportunities for cost cutting are significant; BYOD is an easy way to bring new devices into school without the costs of purchasing or maintaining them.

> "Technology is a tool alone and it is for parents and teachers to help them learn about how to put it to good use"

Beverley Seddon: The switch to e-learning and device-based lesson planning – including BYOD – has been one of the defining changes in teaching practice of recent years.

But while the school gates may be safely shut and security protocols well-rehearsed, Wi-Fi access threatens to throw open a door to the outside world. Friendly WiFi is an accreditation service initiated by the UK Government in 2014 to ensure public Wi-Fi meets minimum filtering standards, particularly in those areas where children are present.

Graeme Lawrie: A blend of reliable Wi-Fi, school equipment and BYOD gives our students secure online access with a degree of autonomy. Aiming for 'any time, any place, any device' access to school systems, we let students choose how they work during the school day and in the evenings. We can't stop students reaching the internet with 3G and 4G access, but we can make it easy for them to connect easily to light-touch, good Wi-Fi that is filtered by content, age of student and time of day. We can, of course, all model good use of technology, as well as setting and enforcing boundaries.

Q. Will children always be one step ahead?

Laura Knight: Not at all, and I am not sure it is reasonable to assume that children are always a step ahead now! Children may be able intuitively to put new technological tools to use (sometimes only in relatively narrow ways) but they do not necessarily have mature judgement. The technology is a tool alone and it is for parents and teachers to help them learn about how to put it to good use. Parents who have grown up with social media may feel this even more strongly!

Henry Seddon: Children will remain ahead in technology because they are more open to it. Children and teenagers especially have a desire to learn, challenge and explore. This results in children adopting technology through apps much more quickly than parents and teachers.

Sarah Williamson: As well as being prime beneficiaries of the digital revolution, children have also been part of a massive, unregulated experiment. It will be interesting to see whether and how the internet can learn to protect children better from harmful content. App developers, for example, are beginning to exploit technologies like AI to guide children's choices online. Ultimately young people will always to need to learn how to temper curiosity with evaluation and control. ET

Main image © depositphotos.com

KEY COMPONENTS FOR A SUCCESSFUL ESAFETY STRATEGY IN SCHOOLS

Al Kingsley, Group Managing Director of NetSupport Limited, talks about school safeguarding solution, NetSupport DNA

It's essential that schools and trusts have the tools to keep their students safe and secure as they access online resources for learning. It would be easy to restrict everything that could be seen as a risk, but, in reality, that's impractical and would impact learning. Fortunately, NetSupport DNA is designed to promote digital monitoring and to encourage students to act responsibly online.

MONITOR INTERNET ACTIVITY

Internet metering is the first step to effective safeguarding, so we provide a detailed summary of all internet activity on each PC by a student, including start and finish times for each website visited and the active time spent on a page. You can manage internet usage fully with lists of approved and restricted website lists to allow options such as: unrestricted access to all websites; restricted access to certain websites that have been marked as approved by the school (such as gaming sites after core school hours); or by completely blocking access to inappropriate sites, where necessary.

MONITOR KEY WORDS AND PHRASES

This sophisticated feature provides schools with insight into (and alerts from) any action by a student that might suggest they are engaged in activity that would place them at risk.

Using a database of pre-supplied safeguarding keywords and phrases covering a range of areas from self-harm, bullying and racism through to risks of radicalisation, NetSupport DNA monitors the network for rogue words. Using advanced neurolinguistics technology to ensure accurate detection (and avoid unnecessary false alarms), it will act on each triggered keyword (by logging the activity, or taking a screenshot or a video recording, depending on the severity of the term) – so you'll know the full background to an event.

TRACK AND REPORT ON TRENDS AND TOPICS

An innovative, easy-to-read word cloud highlights trending topics and helps you to put incidents into context. By clicking on any word in the cloud, you'll see details of which students have typed it and the application used. Language packs are also included (as standard) to support schools with students learning English as an additional language (EAL) and allow safeguarding leads to extend safeguarding provision to an even wider group of students.

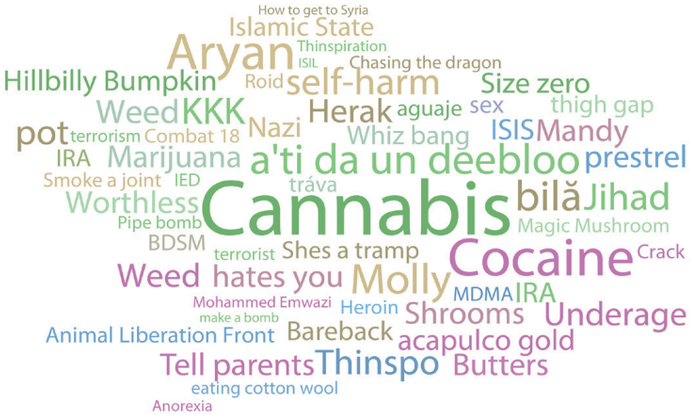
REPORTING CONCERNS

Ensuring students can share any worries they might have is central to any effective safeguarding policy. NetSupport DNA includes a way for them to reach out in confidence to a trusted member of staff via the Report a Concern option. Students can share their problem by sending a message, screenshots (e.g. to show examples of social media-related bullying) or documents to their chosen staff member. The member of staff is instantly alerted when a concern is raised and can then track it and record any follow-up actions directly – with the system alerting if any concern is not actioned within a pre-defined period of time. The key to this feature is to offer simplicity and ease of access for students – backed up by built-in safeguards to guarantee its effectiveness.

MEETING KCSIE AND PREVENT GUIDELINES

By ensuring our safeguarding module reflects the requirements of statutory guidance such as 'Keeping Children Safe in Education' and the Prevent duty, schools can be confident that they are complying with their obligation to safeguard students according to best practice when they choose NetSupport DNA. ET

To find out more about how NetSupport DNA can help your school or academy trust, please visit www.netsupportdna.com/education



Above: Word cloud shows trending topics across a year group or whole school
Below: The dashboard provides an easy-to-read summary of safeguarding events