COMPLIANCE *isn't enough*

Andrew Longhurst explains why 'cyber awareness' alone won't adequately prepare schools for the decisions they need to make around online safeguarding...

Each year, schools across the UK complete the National Cyber Security Centre's cyber security awareness training, in accordance with the DfE's Cyber Security Standards (see tinyurl.com/ts154-CS1). The module takes around 36 minutes to finish, and concludes with the awarding of a certificate confirming completion.

From a governance perspective, this provides reassurance. Schools can evidence that training has been delivered, and that the requirements made of them have been met, but genuine safeguarding operates at a different level — one defined by the quality of decisions made in real situations.

Active decision-making

The government's Keeping Children Safe in Education guidelines (see tinyurl.com/ts154-CS2) make clear that safeguarding isn't just confined to policy or procedure, but also encompasses the ability of staff to recognise risk, interpret context and engage in active decision-making – often under intense time pressures, and with incomplete information.

As time has gone on, safeguarding situations have increasingly come to involve digital systems, communication platforms and information handling. Cyber incidents in schools are rarely confined to technical disruption. Instead, there's a strong likelihood of your safeguarding records, attendance monitoring, financial systems and/or sensitive pupil information being affected.

In an environment where digital systems now underpin safeguarding processes, the quality of staff decision-making in the moment thus becomes as important as the policy itself.

> **"A certificate confirms exposure to information, but not how that information will be interpreted under pressure"**

The question is not whether the existing training is useful. It clearly is. The more relevant question is whether a single annual awareness module, on its own, can adequately prepare staff to make safeguarding-aligned decisions in practice. To understand this, it helps to first look at what the training actually provides.

An awareness baseline

The NCSC module establishes a clear awareness baseline. It explains common threats, such as phishing, ransomware, insider misuse and data loss. It outlines why schools are attractive targets, and uses case studies to show how everyday decisions can lead to cyber security incidents. It then concludes with simple guidance – defend against phishing, use strong passwords, secure devices and report any concerns.

Taken together, this provides structured and accessible awareness. It introduces risk and reinforces basic digital hygiene. It's not designed to test applied judgement or simulate real situations, but to ensure staff understand the fundamentals. And in that context, it capably fulfils its role.

Where the gap emerges is in the difference between 'compliance' and 'competence'. Compliance indicates whether training has been delivered. *Competence* determines whether secure judgement can be applied when it matters.

A certificate confirms exposure to information, but not how that information will be interpreted under pressure, nor how it will be applied when circumstances are unclear.

Consider the following situation. A member of staff receives an email appearing to be from a parent, requesting updated contact information due to an urgent safeguarding issue. The tone fits previous communication, the request feels legitimate and time-sensitive, and nothing about the email feels obviously suspicious.

The staff member has completed the training, knows what phishing is and understands the importance of exercising caution. However, the decision being made here isn't simply, '*Is this phishing?*' – it's '*Do I act now to support a safeguarding concern, or pause to verify and risk delaying something urgent?*' That's what the gap looks like.

Many cyber incidents in schools begin not with obvious warning signs, but with small, reasonable decisions made in good faith, often repeated across similar situations. It might start with opening a seemingly routine attachment, responding to a request that aligns with ongoing work or sharing information in response to an apparently legitimate need.

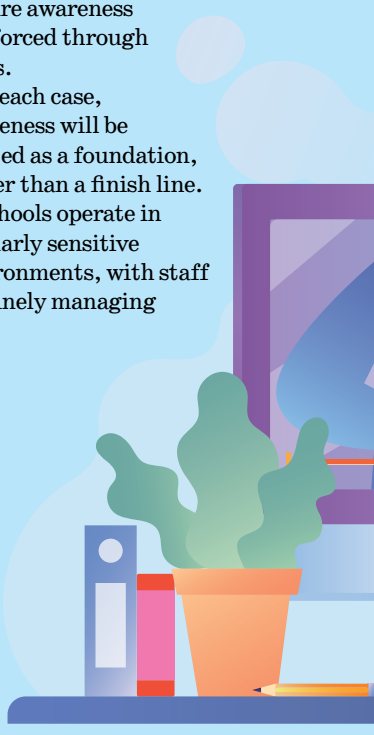
Each of those decisions will have made sense at the time, which is precisely what makes such situational awareness so important.

Evolving threats

This isn't unique to education. In healthcare, infection control training is regularly reinforced through observed practice. In financial services, fraud awareness is supported by simulations and scenario testing. General health and safety practice will see fire awareness reinforced through drills.

In each case, awareness will be treated as a foundation, rather than a finish line.

Schools operate in similarly sensitive environments, with staff routinely managing



safeguarding records, confidential pupil information and daily communications that can carry welfare implications. When digital compromises intersect with safeguarding imperatives, the consequences can be serious.

A compromised parent account requesting information may overlap with safeguarding concerns. A ransomware incident affecting attendance systems can delay the identification of persistent absence. A routine request can introduce ambiguity into situations already requiring careful judgement.

At the same time, the threat landscape has evolved. The current NCSC module has been available since 2021, and while its core principles still remain valid, the environments in which those principles operate have changed.

Generative AI now enables attackers to produce well-written, context-aware messages that can convincingly mirror the tone of professional communications. What were once obvious warning signs are now becoming less obvious.

Verification habits

As the presentation of phishing attacks continues to improve, detection will come to rely less on spotting errors and more on applying consistent verification habits – something that will require both confidence and reinforcement, rather than awareness on its own.

This is where safeguarding expectations and cyber risks can start to overlap more directly.

If safeguarding requires staff to interpret context, assess risk and act appropriately, then digital incidents can't be treated as separate technical events. They have to form part of the same decision-making landscape.

Yet despite this, cyber awareness training tends to be delivered outside of a safeguarding context, with the result being that digital incidents are more likely to be perceived as IT issues, rather than situations that could involve acute safeguarding implications.

Awareness introduces concepts and explains what staff should look for, but it doesn't embed appropriate and consistent staff behaviours when under pressure. In practice, decisions are made mid-task, amid familiar workflows and often under pressing time constraints. When urgency and familiarity are factored in, people will rely on judgement shaped by experience, not just training – which is why awareness, on its own, doesn't reliably translate into confident decision-making under pressure.

Create space for staff

The NCSC module should be seen as a valuable baseline that establishes shared understanding, reinforces expectations and supports compliance. The risks arise only when that *baseline* is mistaken for *completion*.

Safeguarding cultures are layered. Policy provides structure, awareness provides knowledge, and ongoing discussion and reinforcement strengthen judgement. Each layer supports the next.

In practice, this means having to create space for staff to work through real scenarios drawn from everyday school life. That way, decisions can be tested in context and staff can develop the confidence needed to respond well when situations are unclear, time matters and the correct action isn't immediately obvious.

When cyber security is viewed within that context, the issue at hand is no longer whether 'the training has been completed', but whether staff actually feel confident in applying secure judgement when it matters.

Because in modern schools, safeguarding is now inherently digital. Completion can be recorded, but competence can only be revealed in action. Have your staff been fully prepared to recognise and respond confidently when a real safeguarding decision intersects with a cyber incident tomorrow morning? Because that's not a question of compliance – it's a question of leadership.

WHAT GETS MISSED

Most cybersecurity awareness training is designed to be efficient, consistent and easy to complete. Online modules deliver the same content to everyone, to ensure key concepts are covered and compliance requirements are met. What they don't provide is space to explore uncertainty.

If something isn't fully understood when it's introduced – be it phishing, data handling or verification – there are rarely any opportunities to pause, question or work through the area in context. The training continues on the assumption everyone 'gets it', when in practice, they often don't.

Knowledge gaps stemming from concepts that are partially understood or misinterpreted will carry over into later decisions, and without discussion or clarification, they'll persist. This matters, because real situations are rarely clear-cut. When decisions need to be made quickly, people fall back on what *they believe they understand*, which might not be what was intended.

Without chances to test and refine their understanding, trainees can claim 'completion', but still exhibit uncertainty just when their judgement matters most.

ABOUT THE AUTHOR
Andrew Longhurst is Director of Training And Development at the cybersecurity consultancy Cyber Rebels; for more information, visit cyber-rebels.co.uk