

Why School Cyber Security Is Now a Procurement Priority

30 April 2026



For years, cyber security sat near the bottom of the school procurement agenda. Budgets were tight, threats felt distant, and the assumption often unspoken was that schools simply weren't interesting targets.

That assumption is no longer defensible.

The government's Cyber Security Breaches Survey 2025/2026, published this week, confirms what IT managers and school business leaders have been experiencing on the ground: cyber attacks on UK schools are not only common, they are accelerating. Nearly three quarters of secondary schools reported a breach or attack in the last 12 months. For further education colleges, the figure rises to 88%. For universities, it is 98%. And critically, the damage being done is getting worse. One in ten schools now reports critical damage from attacks — up from just six percent the previous year.

What the Numbers Actually Mean

Statistics about cyber attacks can feel abstract until you consider what they mean in practice. Schools that experience ransomware attacks lose access to admin systems, lesson resources, and student records — sometimes for weeks. Teachers have described losing entire classes' coursework overnight. In some cases, schools have been forced to close temporarily while systems are rebuilt from scratch. A single phishing email — the most common attack vector, reported by

96% of secondary schools that experienced a breach — can give a criminal access to financial records, safeguarding files, and the personal data of thousands of pupils and staff. The consequences extend well beyond the IT department. A serious cyber incident means disruption to teaching, potential GDPR breach notifications to the ICO, reputational damage, and significant recovery costs — all falling on a school that almost certainly has no dedicated cyber security budget.

Schools Are Being Targeted — and Criminals Know It

The scale of attacks on schools is not accidental. Education is one of the UK's most consistently targeted sectors, and schools are attractive for a specific set of reasons. They hold large volumes of sensitive personal data — on children, families, and staff — which has significant value on criminal marketplaces. They often run outdated infrastructure that is difficult to patch and maintain on limited budgets. Staff turnover is high, meaning security awareness training has to be continuous to be effective. And unlike hospitals or financial institutions, schools rarely have dedicated security professionals on site. As one cyber security expert noted, schools face a dragnet of opportunistic attacks sweeping the internet — and their defences are often not equipped to stop even the most basic intrusion attempts. One third of education institutions still lack fundamental protections including antivirus software and strong password policies.

The Procurement Response

The good news is that awareness is improving, and procurement decisions are starting to reflect the urgency. Over 80% of primary schools now have a formal cyber security policy in place, rising to at least 90% across secondary schools, colleges, and universities. More schools are investing in staff training — the proportion of teachers receiving cyber security training rose from 61% to 72% in a single year. But policy documents and training programmes are only part of the answer. Schools need vetted, trusted suppliers who can deliver practical cyber security solutions within the constraints of an education budget — and they need to be able to find those suppliers quickly when an incident occurs or a review is triggered. This is where procurement planning matters. Schools that have pre-approved supplier relationships in place before an incident happens recover faster and spend less. Schools that scramble to find help after an attack pay more and wait longer.

What Schools Should Be Prioritising Right Now

For school business managers and IT leads reviewing their cyber security

procurement, the areas that most commonly expose schools to risk include: Email security and phishing protection — phishing remains the dominant attack method across every tier of education. Filtering, staff awareness training, and simulated phishing exercises are among the most cost-effective investments available. Data backup and recovery — schools that maintain current, accessible backups can restore systems quickly and avoid ransomware demands. Recovery time is the single most important factor in limiting the damage from an attack. Access controls and multi-factor authentication — shared logins and weak password policies remain widespread in schools and represent one of the easiest points of entry for attackers. MFA can block access even when a password has been compromised.

Cyber security audits and vulnerability assessments understanding where a school's weaknesses are before an attacker finds them is fundamental. Independent audits, increasingly available at accessible price points for schools, provide a clear starting point for any improvement programme. Staff training and awareness the majority of successful attacks begin with human error. Regular, practical training not just an annual e-learning module — is consistently cited as one of the most effective defences available.

For Suppliers: A Market That Is Ready to Buy

The scale of cyber risk in UK schools represents a significant and growing procurement opportunity for suppliers in the IT and cyber security space. School budgets are constrained, but cyber security is increasingly ring-fenced as a non-negotiable spend category particularly following high-profile incidents and pressure from governors and trustees to demonstrate resilience. Decision-makers including school business managers, IT coordinators, and CFOs of multi-academy trusts are actively seeking trusted suppliers who understand the education sector and can deliver within its specific operational and financial parameters.

Being visible at the point schools go looking — whether that is after an audit, following a sector-wide news story, or at the start of a new academic year procurement cycle — is what turns awareness into enquiries. School Supply Network connects cyber security and IT suppliers directly with schools, academies, and multi-academy trusts across the UK.

If you want your business in front of school buyers who are actively prioritising this area, [find out how to list your business [here](#)].

Sources: *DSIT/Home Office Cyber Security Breaches Survey 2025/2026; Cyber Security Breaches Survey 2025 Education Institutions Findings; ESET UK Education Cyber Security Research 2026; Ofqual/NCSC Schools Cyber Security Survey 2025.*