Dataspire

Schools and Cyber Security:
Behind the Firewall

What real cyber audits in real schools actually reveal.

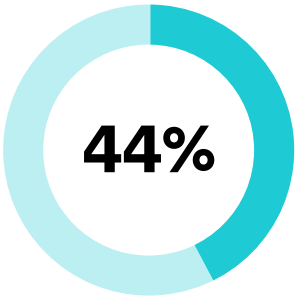
Think Digital Education, Think Digital Transformation, Think Dataspire!

Schools and Cyber Security:

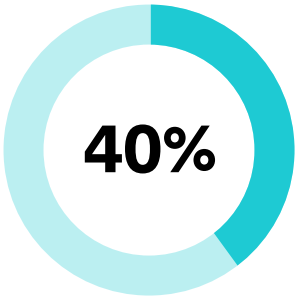
Behind the Firewall

What real cyber audits in real schools actually reveal.

Based on findings from schools audited by Dataspire as part of the DfE Cyber Security Standard pilot programme.



Average overall fail rate



Average critical fails per school

Schools with at least one critical gap

Section 1: Introduction

Cybercrime isn't a distant threat for UK schools. It's happening now, right across the sector, and the numbers are hard to ignore.

In the past 12 months, 60% of secondary schools and 44% of primary schools identified a cyber security breach or attack. Both figures are higher than the 50% reported by UK businesses overall, which means schools are being targeted more than the average commercial organisation, despite having fewer resources to defend themselves.

Recovery costs from ransomware attacks can stretch into the millions, money that could otherwise be spent on teaching, learning resources, or safeguarding programmes. **Ransomware incidents alone have cost UK schools up to £3 million per event, with ransom demands ranging from £50,000 to over £5 million.**

But the disruption goes beyond money. **Systems can be taken offline for weeks, exam materials become inaccessible and staff get locked out of pupil data.** Over a third of English schools were hit by cyberattacks in 2024, some of which forced systems offline for weeks.

Yet, despite the scale of the threat, most schools still have significant gaps in their defences. **One in three UK educational institutions still lacks fundamental protections such as antivirus software and strong password policies.** The majority have not adopted advanced measures like managed detection and response, and we completely understand that this isn't merely negligence, but more a combination of stretched budgets, competing priorities, and simply not knowing where the gaps are.

So that's where we come in.

Why Dataspire produced this report

Dataspire has been working with schools on IT and cyber security since 2005. In that time, we've seen the threat to schools grow from an occasional concern into a persistent operational risk. We've also seen schools struggle to get a clear picture of where they actually stand, not because they don't care, but because honest, independent assessment is hard to come by.

Of course, you trust your IT support, but they're overwhelmed and either don't want to disappoint you or are reticent to ask for additional resources.

In 2025, we were selected by the Department for Education as 1 of 6 pilot partners for the DfE Cyber Security Standard programme. That means we've been working directly alongside government to help define what good cyber security looks like for schools and auditing schools against that standard in the field.

This report shares what we found. Not to scare, but because the data is striking enough that school leaders need to see it, and because transparency about the real state of school cyber security is more useful than another generic guide telling you to "change your passwords."

The schools in this report aren't unique, they're representative of your peer schools, and if you're a Headteacher or Business Manager reading this, there's a reasonable chance your school could look similar.

Section 2: About this report

This report draws on findings from schools audited by Dataspire as part of the Department for Education's Cyber Security Standard pilot programme. *Every figure in this report comes directly from those audits. Nothing has been inferred or estimated.*

Each audit assessed schools across six security themes, covering over 150 individual checks. Findings were recorded against the DfE Cyber Security Standards, with each check marked as Pass, Fail, or Not Applicable. Where a check was marked as Critical and the school failed, that failure is counted as a Critical Fail throughout this report.

School names have been removed. All data is presented in aggregate to protect the schools involved and to give an honest picture of the sector rather than single out individuals.

Schools Audited

Schools were audited across six security themes, covering primary, secondary, and all-through phases.

Audit framework

The DfE Cyber Security Standard, assessed across ***Physical Security, Infrastructure Configuration, Governance and Risk, Planning, Operational Protection, and Vulnerability Management.***

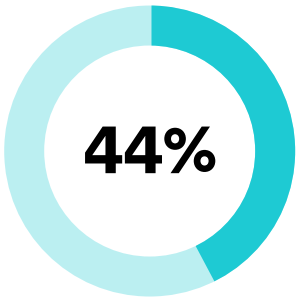
Who conducted the audits

Dataspire's technical team, working as a DfE pilot partner for the Cyber security Standard programme.

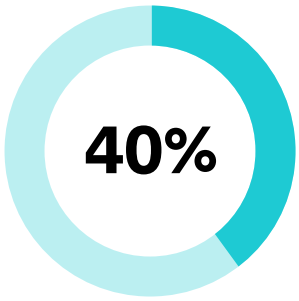
Section 3: The Numbers

Across the individual checks, the average overall fail rate was 44%. That means nearly half of everything we looked at wasn't in place. **The best-performing school failed 24% of checks. The worst failed 67%.**

Every single school had critical gaps and not one passed everything.



Average overall fail rate



Average critical fails per school

Schools with at least one critical gap

Section 4: What we found, theme by theme

The audits covered six security areas. Here's what we found in each one, ordered from the highest to the lowest fail rate.

Vulnerability Management - 79% fail rate

The highest fail rate of any theme. Most schools had no formal process for identifying, tracking, or fixing vulnerabilities in their systems.

- **89%** schools had no Vulnerability Management Policy
- **89%** had no plan for zero-day vulnerabilities
- **78%** had no vulnerability scanning tools
- **78%** produced no vulnerability reports for leadership
- **67%** had no asset discovery capability

What this means

If something goes wrong with a system in your school, who finds out first, you, or the person who's already exploited it? **Without vulnerability management, most schools wouldn't know they had a problem until it became an incident. This is a gap in the school's ability to protect its own data and operations.**

Planning - 46% fail rate

Schools were missing the plans, logs, and processes that would let them respond effectively if something went wrong.

- **89%** hadn't established data classification procedures for incidents
- **78%** had no cyber risk log
- **67%** hadn't carried out a cyber risk assessment in the last 12 months
- **67%** hadn't completed a business impact analysis
- **67%** not fully DfE Cyber Standards compliant

What this means

A cyber incident isn't just an IT problem, it can knock out systems for days, prevent access to pupil data, and in serious cases lead to regulatory action. The schools that recover fastest are the ones that planned for it before it happened. Most of the schools we audited hadn't.

Governance and Risk - 42% fail rate

Cyber security wasn't being treated as a leadership responsibility. In most schools, it was being handled informally, if at all.

- **67%** had no cyber risk register
- **67%** didn't discuss cyber at board level
- **56%** had no named governor responsible for cyber
- **56%** had risks with no assigned owners or tracked actions
- **78%** couldn't confirm suppliers held CE + / CAF / ISO assurance

What this means

The DfE is explicit: cyber governance is a leadership responsibility, not just an IT one. Academy trusts in particular are required to have proportionate controls under the Academy Trust Handbook. When there's no named owner, no risk register, and no board visibility, there's no accountability and no early warning when things start to go wrong.

Operational Protection - 41% fail rate

Day-to-day protective measures were inconsistently applied. Key monitoring and patching controls were missing in the majority of schools.

- **78%** not monitoring internal network traffic for unusual patterns
- **78%** had no patching or software audit solution
- **56%** running legacy OS or software
- **58%** cloud/SaaS backups not tested or reviewed

What this means

Patching is one of the most basic cyber hygiene actions a school can take, and most schools weren't doing it consistently. Legacy software is one of the most common entry points for attackers. Not monitoring internal traffic means that even if someone is already inside the network, the school wouldn't know.

Infrastructure Configuration - 37% fail rate

Network infrastructure had significant configuration gaps, leaving more room for attacks than necessary.

- **100%** schools had no 802.1X/RADIUS network authentication (user/device verification)
- **78%** had unused switch ports that weren't disabled
- **67%** not using Protected DNS (PDNS - Protected Domain Name Service)
- **56%** not analysing firewall logs for anomalies

What this means

An open switch port or an unprotected network segment is basically a door that anyone in the building could walk through. Not one school had 802.1X authentication in place, meaning that connecting to the network required no individual user verification at the network level.

Physical Security - 19% fail rate

The best-performing area, though critical fails were still present in most schools, particularly around server room access and switching equipment.

- **Some schools had servers in unsecured or accessible locations**
- **Network switching equipment was physically accessible in corridors in several schools**

What this means

Physical access to a server or a switch can bypass almost every digital control you've put in place. It's the one area that's hardest to remotely monitor and easier to overlook because it doesn't feel like a 'cyber' issue, but it is.

Section 5: The findings that surprised us most

Some findings were predictable, however these were not.

100% - No 802.1X/RADIUS network authentication

Not one school had 802.1X/RADIUS network authentication in place. This means any device connected to the network wasn't individually verified at the network level.

89% - No Vulnerability Management Policy

These schools had no Vulnerability Management Policy and no plan for zero-day threats. Zero-day vulnerabilities are actively exploited before patches exist. Without a policy, there's no process to respond.

78% - No internal network traffic monitoring

These schools weren't monitoring internal network traffic for unusual behaviour. Most cyber incidents are only discovered after the damage is done. Monitoring is how you catch them earlier.

67% - Not fully DfE Cyber Standards compliant

These schools weren't fully compliant with the DfE Cyber Standards, despite the 2030 deadline approaching. ***Non-compliant schools risk losing RPA cyber cover eligibility.***

67% - Cyber not a standing board agenda item

Cyber security wasn't a standing agenda item at board or leadership level in these schools. Without regular governance oversight, there's no mechanism to drive improvement or ensure accountability.

The Good News:

100% - All schools had key policies reviewed and communication plans in place

Despite everything above, all schools had key policies reviewed and alternative communication plans in place. This shows it's not a question of intent, the gaps are in implementation and technical controls, not awareness that security matters.

Section 6: What good looks like

The DfE Cyber Security Standard sets out what schools should have in place. The schools that performed better in our audits shared a set of common characteristics.

Importantly, the best-performing school in our sample didn't have a bigger budget or a larger IT team. They had clear ownership, more consistent processes, and leadership that treated cyber security as an operational priority rather than an IT department problem.

Named ownership at leadership level

A designated SLT member with explicit responsibility for cyber risk, not just an IT technician managing it informally.

Cyber on the board agenda

Regular governance discussions, at least termly, with a named governor for cyber/digital risk.

A live, maintained risk register

Risks documented, owned, and reviewed, not a one-off document sitting in a shared drive.

Tested backup and recovery processes

Backups are only useful if you know they work. Better-performing schools had tested their recovery processes.

Consistent patching and update processes

Security updates applied promptly across all devices and systems, with someone accountable for it.

Staff awareness training completed and evidenced

Not just a once-a-year email, but training with records to show it happened and who completed it.

Section 7: Where to start

If you're reading this and recognising your school in some of these findings, the good news is that the highest-impact actions aren't necessarily the most expensive ones.

1. Establish clear ownership

Appoint a named SLT member with explicit responsibility for cyber security. Put cyber on the board agenda at least termly. This costs nothing and changes everything about how the issue gets managed.

2. Build and maintain a cyber risk register

You can't manage what you haven't identified. A risk register doesn't need to be complicated, it just needs to exist, be maintained, and have named owners against each item.

3. Test your backups

This is one of the four conditions for RPA cyber insurance eligibility. If you can't restore from a backup, having one doesn't help you. When did your school last test a restore?

4. Get your patching under control

Unpatched systems are one of the most common entry points for attackers. Know what's running in your school, know what version it's on, and have a process for keeping it up to date.

5. Get an independent audit

You can't self-assess your way to a clear picture of your cyber security. An **independent audit** against the DfE standard will tell you exactly where you stand and what needs addressing first.

Section 8: Is your school in the same position?

The schools in this report weren't unique, they're representative of what we see across the sector. If you're not sure where your school stands against the DfE Cyber security Standard, the only way to find out is to look and the best way to understand what you're working with and where to begin is with Dataspire ONE Secure.

What is Dataspire ONE Secure?

With this data we've been able to create a solution that supports schools on their security journey while fixing the exact problems that you're facing. **We haven't just made up a solution that we think will work, we've developed something based on your needs and we did that alongside you.**

How it works:

We'll begin with an audit, just like the ones delivered above to ensure that the DfE Standards are reflected in your outcomes.

We'll share your findings and then assign you a designated account manager who will engage with you on a (Termly basis) to see where you have made improvements and where gaps may have widened.

Your account manager will be the bridge between your IT team and SLT, helping to translate and arrange the work that is necessary (in order of priority) to meet the standards and get you on track.

It doesn't have to be done all at once, and once improvements have been made, over a set period of time, we can work with you to get your official Cyber Essentials accreditation.

Ready to find out where your school stands?

If you'd like to know how your school compares, we'd be glad to help. **Dataspire ONE Secure gives you a clear, honest picture of where you stand against the DfE Cyber Security Standard, what your critical gaps are, and where to focus first.**

Speak to our team today.

info@dataspire.co.uk | 0345 603 1233 | dataspire.co.uk

SOURCES:

- *Cyber-security-breaches-survey-2025-education-institutions-findings*
- *Rising-cost-of-cyber-attacks-on-uk-schools-what-you-need-to-know*
- *Classrooms-in-the-crosshairs-ransomwares-growing-threat-to-schools/*
- *Schools-hit-by-cyberattacks*

Dataspire

info@dataspire.co.uk | 0345 603 1233 | dataspire.co.uk