Dataspire

Cyber Security *for School Governors*

What you need to know, what questions to ask, and how to keep it on the agenda.

Think Digital Education, Think Digital Transformation, Think Dataspire!

Cyber Security *for School Governors*

What you need to know, what questions to ask, and how to keep it on the agenda.

This guide is written for governors and trustees of schools and academy trusts.

You don't need a technical background to read it.

The goal is to help you understand your responsibilities around cyber security, know what good looks like, and make sure the right conversations are happening at board level.

Why cyber security is now a governance issue

Not long ago, cyber security was seen as something for the IT team to deal with but that has changed. The Department for Education, the Academy Trust Handbook, and the wider regulatory environment are now clear:

Cyber security is a leadership and governance responsibility, not a technical one.

That doesn't mean governors need to understand firewalls or configure networks, but it does mean the board needs to be asking the right questions, receiving the right assurance, and ensuring the school has the right controls in place.

According to the government's Cyber Security Breaches Survey 2025**, 60% of secondary schools and 44% of primary schools identified a cybersecurity breach or attack in the past 12 months**, both figures being higher than the 50% reported by UK businesses overall. **Schools are being targeted more than the average commercial organisation,** despite having fewer resources to defend themselves.

The consequences are serious. Ransomware incidents have reportedly **cost individual schools up to £3 million. Systems have been taken offline for weeks.** Pupil data, (names, addresses, medical records, safeguarding information) has been stolen and threatened with public release.

This is the context in which governors are now being asked to provide oversight.

WHAT THE DFE SAYS

The DfE's Governance Guide (published March 2024) introduced new (and continued) advice that at least one governor or trustee should complete cyber security training (paragraph 7.7.3 for maintained schools, paragraph 7.9.3 for academies). For academy trusts, the Academy Trust Handbook 2025 states that trusts must be aware of the risk of cybercrime, put in place proportionate controls, and take appropriate action where a cyber security incident has occurred (section 6.14).

What governors are responsible for

Your role isn't to manage cyber security day to day, it's to ensure that the school's leadership team is doing so effectively, and to provide strategic oversight and accountability.

In practice, that means the governing board should be:

- ensuring there is a named member of the Senior Leadership Team with explicit responsibility for cyber security
- ensuring at least one governor or trustee has completed cyber security awareness training
- receiving regular reporting on the school's cyber posture and any incidents
- satisfied that the school's cyber risk is documented, owned, and being managed
- ensuring the school has a tested incident response and business continuity plan
- checking that the school is working towards compliance with the DfE Cyber Security Standards by 2030

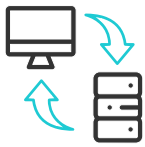
ACADEMY TRUSTS: AN ADDITIONAL OBLIGATION

If you are a trustee of an academy trust, your obligations go further. Section 6.14 of the Academy Trust Handbook 2025 requires trusts to put in place proportionate controls against cybercrime and take appropriate action where an incident has occurred. Trusts are also explicitly directed to meet the DfE's published cyber security standards.

The RPA and why it matters

Many schools use the Risk Protection Arrangement (RPA). RPA is the government's alternative to commercial insurance, rather than a commercial policy. If your school does, there are four specific conditions it must meet to be eligible for cyber cover.

These conditions, as set out by the DfE, are:



1. Offline Backups

The school must meet the DfE's cyber security standard for backups, which requires at least three copies of important data, on at least two separate devices, with at least one stored offsite.

2. Annual Cyber Security Training

All employees and governors who have access to the school's IT systems **must complete the NCSC's cyber security training** for school staff annually.

3. Registration with Police CyberAlarm:

The school must be registered with the Police CyberAlarm tool (Note: registration is the requirement, not installation of the software).

4. A Cyber Incident Response Plan:

A documented plan for contingency and recovery in the event of a cyber-attack must be in place.

As a governor, it's reasonable to ask for written confirmation that all four conditions are met and when they were last reviewed. If they can't be evidenced, the school may not be covered in the event of an incident.

IMPORTANT: THE RPA DOES NOT COVER RANSOM PAYMENTS

The DfE's position, in line with National Crime Agency and NCSC advice, is that ransom payments should not be made. The RPA will not cover ransom payments or expert fees to investigate threats relating to ransom demands. This makes prevention, and having a tested recovery plan, all the more important.

What good governance looks like

Based on the DfE Cyber Security Standards and our own audit experience, here's what well-governed schools have in common when it comes to cyber security.

Clear Ownership

There is a named SLT member with explicit responsibility for cyber security, not just an IT technician. That person reports to the board and can be held accountable. There is also a named governor or trustee with responsibility for cyber risk oversight.

A Live Risk Register

Cyber risk is documented in the school's risk register, with named owners against each risk and a clear record of what's being done to address it. It's reviewed at least annually, ideally more frequently.

Regular Board Reporting

The board receives a cybersecurity update at least once a term. This doesn't need to be lengthy, a short written report covering the current risk position, any incidents, and progress against the DfE standard is sufficient.

An Incident Response Plan

The school has a documented plan for what happens if a cyber incident occurs, who is contacted, what systems are taken offline, how the school communicates internally and externally, and how it recovers. This plan has been tested, not just written.

Tested Backups

The school backs up its data regularly, meeting the DfE standard of at least three copies, on at least two devices, with at least one stored offsite and has tested whether it can actually restore from those backups. A backup that hasn't been tested is not a backup, it's hoping for the best.

Annual Staff Training

All staff who access school systems receive the NCSC's cyber security awareness training at least annually. This is evidenced and there are records showing who completed it and when. At least one governor or trustee has also completed training.

Questions to ask at every board meeting

You don't need to be a cyber security expert to hold the school to account on this. You just need to ask the right questions and expect clear answers. If the answers are vague, that's a finding in itself.

The following questions are a starting point. They're written in plain English because that's how board conversations happen.

Questions about governance and ownership

- **Who in our SLT is responsible for cyber security?**
- **What does that responsibility include?**
- **Which governor or trustee has oversight of cyber risk?**
- **Have they completed cyber security training?** Yes/No
- **Is cyber risk on our risk register?** Yes/No
- **Who owns it, and when was it last reviewed?**
- **When did we last receive a cyber security update at board level?**

Questions about compliance and standards

- **Are we working towards the DfE Cyber Security Standard or Cyber Essentials?** Yes/No
- **Where do we currently stand?**
- **If we use the RPA, can we evidence that all four eligibility conditions are met?** Yes/No
- **Have all staff who access school systems completed the NCSC cyber security training in the last 12 months?** Yes/No
- **Have we had an independent audit of our cyber security in the last two years?** Yes/No

Questions about resilience and response

- **Do we have an incident response plan? Yes/No**
- **When was it last tested?**
- **Do our backups meet the DfE standard (at least three copies, two devices, one offsite)? Yes/No**
- **When did we last test a restore?**
- **If our systems went down tomorrow, what's our plan for communicating with staff, parents, and pupils?**
- **Have we had any incidents or near-misses in the past 12 months? Yes/No**
- **What did we learn from them?**

A NOTE ON "I'LL CHECK WITH IT"

If questions about cyber risk are consistently met with "I'll check with IT" or "our IT provider handles that," that's worth probing further. Cyber security is a leadership responsibility.
vThe IT team or provider implements controls, but the board should be receiving assurance that those controls are in place and working, not just assuming they are.

How often should cyber be on the agenda?

Cyber security doesn't need to be a lengthy agenda item at every meeting but it does need to be a standing item, meaning it appears regularly, with a consistent owner and a clear expectation of what's being reported.

The table below sets out a suggested framework for governing boards.

Agenda item	Suggested frequency	Who leads
Cyber security risk update: Current posture, any incidents, progress against DfE standard	Termly	SLT digital lead
Risk register review: Cyber risks reviewed, owners confirmed	Termly	SLT digital lead/ Headteacher
Staff training completion: Confirmation all staff have completed NCSC training in the last 12 months	Annually	SLT digital lead
Incident response plan review and test results	Annually	SLT digital lead/ IT
Backup standard confirmation: Three copies, two devices, one offsite, restore tested	Annually	IT provider/ SLT digital lead
RPA eligibility review: All four conditions evidenced (if applicable)	Annually	Business Manager/ Headteacher
Independent audit findings (if applicable)	As required	Headteacher/ Business Manager
DfE Cyber Standards compliance progress towards 2030 or Cyber Essentials	Annually	SLT digital lead

If your board doesn't currently have a standing cyber agenda item, a practical first step is to ask the Headteacher or Business Manager to bring a short written update to the next meeting. That creates the habit, establishes the expectation, and gives the board a baseline picture to work from.

What to do if you have concerns

If you ask these questions and the answers suggest your school isn't where it should be, that's not unusual. Our audit data shows that most schools have significant gaps, the important thing is that the board is aware and that there's a plan to address them.

If your school hasn't had an independent audit

An ***independent audit*** **against the DfE Cyber Security Standard or Cyber Essentials** is the most reliable way to understand where the school actually stands. Self-assessment has its limits, an external (and unbiased) audit gives the board genuine assurance, and gives the SLT a clear prioritised list of what needs addressing.

If there's no named SLT lead for cyber security

Raise it at the next board meeting. Ask the Headteacher to identify who in the leadership team will own this responsibility and what that ownership includes. It doesn't require a new post, it requires clear accountability within the existing structure.

If the risk register doesn't include cyber security

Ask for it to be added before the next meeting, with a named owner and an initial assessment of the school's current exposure. A cyber risk entry doesn't need to be complex, you just need to have one in place.

If staff training hasn't happened

The NCSC provides free cyber security training for school staff and governors through its online platform. Your Business Manager or SLT digital lead can organise this. The board should receive confirmation of completion and all staff who access school systems should complete it annually.

Raise it at your next board meeting.

If anything in this guide has prompted questions you can't yet answer about your school's cyber security, that's exactly what it's designed to do. Share this guide with your Headteacher or Business Manager and put cyber security on the agenda for your next meeting.

If your school hasn't had an **independent audit** against the DfE Cyber Security Standard, that's a good conversation to start. ***Dataspire has been working with schools on cyber security since 2005 and was selected by the DfE as 1 of 6 pilot partners for the Cyber Security Standard programme. That means, we're well-placed to give your school a clear, honest picture of where you stand.***

Speak to our team today.

Email info@dataspire.co.uk **or** call 0345 603 1233 and we will help you understand where your school stands against the DfE Cyber Security Standards.

SOURCES:

- *DSIT Cyber Security Breaches Survey 2025*
- *DfE Governance Guide (7 March 2024 & 2025), paragraphs 7.7.3 and 7.9.3*
- *Academy Trust Handbook 2024 & 2025, section 6.14*
- *DfE Cyber Security Standards for Schools and Colleges*
- *DfE Risk Protection Arrangement conditions (gov.uk)*

Dataspire

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