Secure Schools

The school cybersecurity handbook

2024–25

03.

Introduction

The education system is disproportionately affected by threats to cybersecurity

Thank you for downloading the 2024–2025 School Cybersecurity Handbook. My team and I maintain the school cybersecurity handbook programme to organise and consolidate the vast amount of advice and guidance given to schools. At first, this was primarily NCSC guidance to all organisations, but over the last 5 years, we've seen requirements grow from multiple directions; the Department for Education through their Cyber Security Standards and Risk Protection Arrangement, the Education and Skills Funding Agency through the Academy Trust Handbook, and other insurers through conditions of cover. For schools and academy trusts, it's more difficult than ever to establish cybersecurity requirements whilst monitoring new risks as threats also evolve.

Our vision is safe and undisrupted education around the globe, and this Handbook remains one of our most significant contributions to making this a reality.

Our ambition is to make this resource the only document your school needs to align its cybersecurity strategy with regulators' and stakeholders' requirements and expectations. For schools that have already adopted Secure Schools initiatives, we've included guidance on how to use them to meet these regulations and expectations.We wish you a successful, productive, and safe academic year.

Paul Alberry

Co-founder and CEO
Secure Schools

Department for Education

National Cyber Security Centre
a part of GCHQ

Education & Skills Funding Agency

*View source of these statistics

Key trends of 2023–24 academic year

Schools continue to be attacked as they are seen as soft targets with vast amounts of valuable data. However, recent updates in government expectations and high-profile attacks and outages mean that more schools are realising the urgency of cybersecurity and beginning their cyber resilience journey.

1. ### Rising cyber-attacks on schools
   Schools remain prime targets, with a 55% increase in cyber incidents. In 2023-24, 52% of primary and 71% of secondary schools reported breaches, with phishing being the most common attack.

2. ### AI-driven threats
   Hackers are using AI to make phishing emails and vishing calls more sophisticated and harder to detect.

3. ### Protective measures for schools
   Staff training and phishing simulations are crucial but underused: 92% of primary and 89% of secondary schools experienced phishing attacks, yet only 62% and 75%, respectively, conducted phishing simulations.

4. ### Supply chain vulnerabilities
   With increased reliance on technology, securing the supply chain is vital. Schools should have reliable backups and incident response plans, as emphasised by the recent CrowdStrike outage.

5. ### Leadership accountability
   The DfE and ESFA now require a senior leader to oversee cybersecurity, working closely with IT teams. Despite budget challenges, schools are encouraged to adopt low-cost cybersecurity measures.

How to prepare for 2024–25

In response to these trends, government and regulatory bodies are introducing more robust cybersecurity regulations and guidance for educational institutions. The focus has been on protecting students' data, driven by incidents of data breaches and the growing recognition of privacy rights. The DfE's latest cyber security standards and the ESFA's Academy Trust Handbook have a much firmer stance on schools and trusts implementing robust cybersecurity strategies.

In this year's handbook, we will share all you need to know about the latest regulations and guidance for England, as well as the most effective ways to keep your school or trust safe.

06.

*Audits and internal scrutiny

Updated DfE Cyber Security Standards

What's new, and what do I need to do differently?

The updated cyber security standards include more guidance on implementation. These new standards are essential to ensuring the cyber safety of your staff and students.

Here are the critical points for your consideration:

1. ### Appoint a member of the senior leadership team as a digital lead that's responsible for cybersecurity

   Designating a digital lead is key in ensuring the standards are met. Choose someone with suitable authority and who can work with your IT support team.

2. ### Work with your IT support team. If they are external, it is essential that you ask for their support to achieve the standards

   Whoever supplies your IT support, cybersecurity is your responsibility. If your support is external, you must understand what measures are being taken to protect your school. If this isn't clear, ask them how they can help you meet the standards. If your IT support team doesn't have the capacity to support cybersecurity, look for additional support.

3. ### Prepare for the worst

   The standards stress the need to develop, regularly update and rehearse a cyber incident response plan.

4. ### Conduct regular, timely training for your staff and students

   Provide regular cybersecurity training for all staff and at least one governor or trustee, emphasising the importance of recognising phishing attempts and other common threats.

   Traditionally focussed on cyber-safety and cyber-bullying, the updated standards call for student training to encompass cybersecurity.

5. ### Cybersecurity is not a one-off

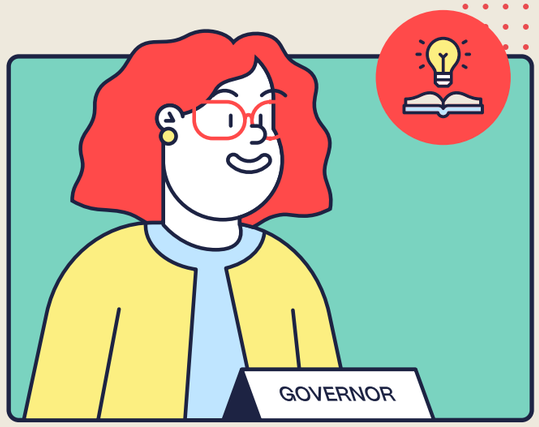
   Conduct regular cybersecurity audits* to assess the effectiveness of current measures and identify areas for improvement. The standards stress the importance of regular testing and ongoing activity to maintain cyber resilience.

07.

How Secure Schools can help you meet updated DfE standards

Secure Schools
School Board Awareness Training

Our School Board Awareness Training will make you or your school governor knowledgeable, compliant, and ready to implement the DfE's updated standards in less than 20 minutes.



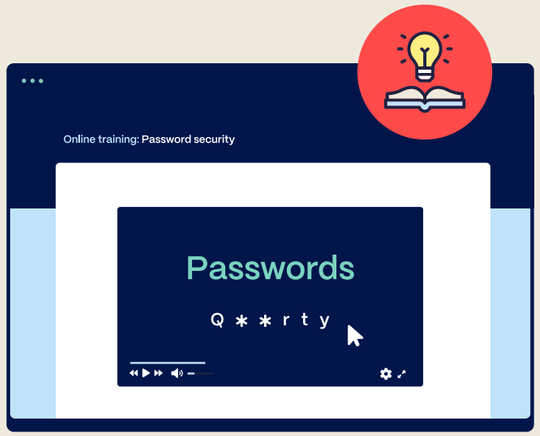
Secure Schools
Cybersecurity Policy Builder

As the DfE Cyber Security Standards includes a comprehensive list of requirements, you'll need to create one of each policy in the Policy Builder to cover all areas of the DfE Cyber Security Standards.

Secure Schools
Cybersecurity Awareness Training

Access these training modules:

- Phishing
- Password security
- Social engineering
- The dangers of removable storage media



Not yet using **Secure Schools**?
Sign up for a **FREE** trial

Click here to sign up

Keeping Children Safe in Education – 2024

Just days after the latest DfE Cyber Security Standards were released, the 2024 Keeping Children Safe in Education report was also published. There is a wealth of valuable information within the report, but we have just focussed on the main 2024 updates regarding cybersecurity here:

1. ## Enhanced online safety measure

The report emphasises the need for schools and colleges to enhance online safety measures, ensuring that children are protected from cyber threats such as cyberbullying, online exploitation, and inappropriate content.

2. ## Updated guidance on cybercrime

The section on cybercrime has been updated to provide clearer guidelines on how schools should address cyber threats and online security issues. This includes recognising signs of cybercrime and appropriate responses to protect students.

3. ## Emphasis on data protection

There is a reinforced focus on compliance with the Data Protection Act 2018 and GDPR, ensuring that schools handle student data securely and protect it from unauthorised access or breaches.

4. ## Integration of digital safeguarding

Digital safeguarding is now integrated into the broader safeguarding framework, highlighting the importance of protecting children in digital spaces as part of their overall welfare.

5. ## Training for staff

The report mandates that staff receive training on cybersecurity and online safety, equipping them with the knowledge to identify and respond to online risks effectively.

6. ## Cybersecurity in safeguarding policies

Schools must update their policies to include specific online safety and cybersecurity provisions, ensuring these are part of the standard procedures for protecting students.

These changes reflect an increased recognition of the importance of cybersecurity in safeguarding children and ensuring their safety in an increasingly digital world. You can read the full report for yourself*.

*Read the report here

How Secure Schools works with you

Have specific requirements?

We work with you to establish how our tools and expertise can support more advanced projects.

What we do

Audit & internal scrutiny

Discover cybersecurity risks and build overall cyber resilience with independent assurance. Our self-evaluation option is a great starting point for your cybersecurity journey.

Phishing simulator

Current and relevant phishing simulations specifically for schools. Our phishing simulations use actual school technologies and examples to be more like the ones hackers send.

Policy builder

Build strategy, policy and a robust cybersecurity plan via our security management platform, an innovative, easy-to-use one-stop solution for school cybersecurity governance, risk, and compliance.

Penetration testing

Test your school's security to identify and confirm your school or trust's cybersecurity strengths and weaknesses.

Online training

Staff-friendly training that's short and snappy, updated annually and aligns to the latest cybersecurity standards.

Our solutions work individually or together to equip educational institutions with the knowledge and tools needed to navigate the complex landscape of cyber threats.

Embrace a proactive approach to cybersecurity, and create a resilient environment protecting both data and the well-being of students and staff.

Get started with Secure Schools

Observed audit trends

What do we find in schools?

Our cybersecurity assessors audit hundreds of schools every year. Here's a summary of their findings and our recommendations for avoiding the risks.

Governance

- Most schools have a risk and audit committee
- Cybersecurity is not a standing meeting agenda item.
- Cybersecurity is included on all board and committee meetings to ensure cyber is prioritised.

72% of schools do not have a named board member responsible for cybersecurity

Vulnerability and patch management

- Most schools use unsupported software or do not keep software up-to-date.
- Unsupported software leaves vulnerabilities open to exploitation by cybercriminals.
- Schools look for alternatives to unsupported software and implement updates within 14 days of release.

75% of schools stated their boards are unaware of when the last vulnerability scan took place, or how regularly they are run

Policies and documentation

- Most schools don't have relevant or up-to-date cybersecurity policies.
- Cybersecurity policies ensure all staff are aware of their responsibilities.

Cyber incident response

- Most schools don't have a cyber incident management plan or don't test it.
- Without one, claims to the RPA could be refused.
- A cyber response plan is also a requirement of the DfE cyber security standards.

Password strategy

- Most schools still use outdated password expiry schedules.
- Multi-factor authentication is growing, with schools implementing it to protect high-value or high-influence accounts.
- The NCSC recommends using MFA and single sign-on instead of passwords. If a password is necessary, they recommend password managers and machine-generated passwords.

Administrative access to systems

- Network administrators are not segregating their day-to-day accounts from administration accounts or they use the same password on both accounts.
- Accounts with higher access or access to higher-value systems can be targeted through spear or whale phishing or compromised through credential stuffing.
- Segregated accounts protected with MFA.

Backing up cloud services

- Most schools wrongly assume cloud vendors take regular data backups.
- Not all cloud vendors regularly back up customer data, and supply chain attacks could render these backups unavailable.
- Backup schedules are checked for all cloud vendors, and schools implement their own backup schedules.

Source: Secure Schools primary consumer research

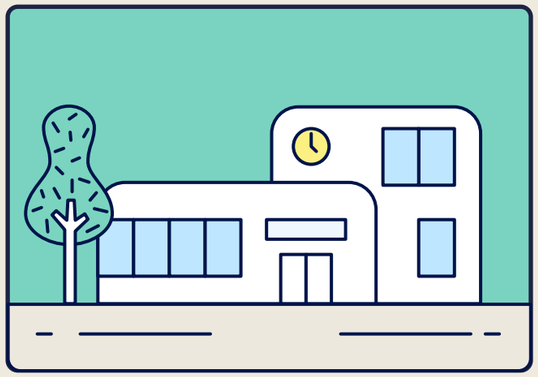
Discover Secure Schools audit and internal scrutiny options

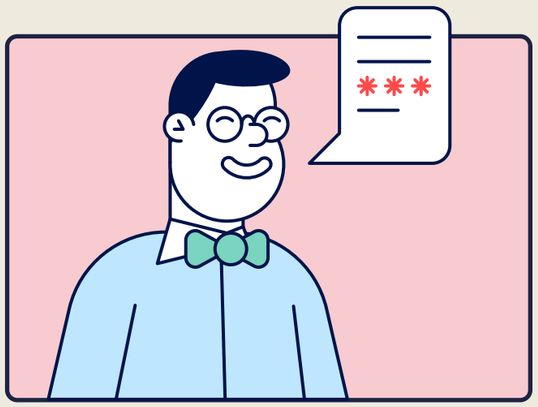
Secure Schools
Cybersecurity Audit

We've developed a standard that represents an appropriate level of cybersecurity for UK schools and trusts, incorporating the latest expectations from the DfE and ESFA, along with guidance from the National Cyber Security Centre (NCSC) and Cyber Essentials and IASME Cyber Assurance standards.

Secure Schools
Internal Scrutiny

The Secure Schools internal audit service is for schools and trusts seeking independent assurance about the security of their information systems, policies and processes. Our unique framework and approach has been developed by industry experts who understand the challenges faced by the education sector.





Secure Schools
Penetration Test

Our expert team of OSCP–certified pentesters ensure that potential threats are identified and can be mitigated before they cause harm, giving you peace of mind and the confidence that your school's cybersecurity measures are robust and effective.

ESFA academy trust handbook

Applies to: All academy trusts in England

The Education and Skills Funding Agency reviews and usually updates the Academy Trust Handbook annually. The Handbook contains cybersecurity-specific requirements, which are becoming increasingly prominent as the sophistication of cyber-threats increase in the education sector.

For 2024, trusts should take appropriate action to meet DfE's Cyber Security standards, which were developed to help them improve their resilience against cyber-attacks.

'Musts' according to the Academy Trust Handbook

The following are cybersecurity requirements of academy trusts according to the Academy Trust Handbook and its Schedule of Musts:

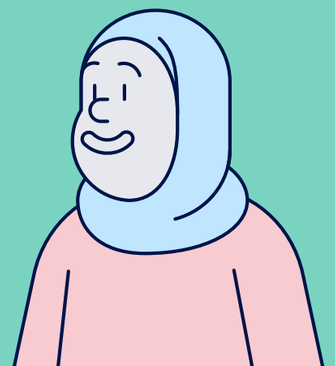
- Academy trusts must be aware of the risk of cybercrime.
- Academy trusts must put in place proportionate controls.
- Academy trusts must take appropriate action where a cybersecurity incident has occurred.
- Academy trusts must obtain permission from the ESFA to pay any cyber ransom demands.

Internal scrutiny

Trusts with annual revenue over £50 million will be expected to "deliver internal scrutiny" over the next academic year by using an in-house auditor or buying in such services. By September 1, 2025, they will be mandated to have these measures in place.

Many academy trusts elect to include cybersecurity as a risk area for internal scrutiny. The Academy Trust Handbook states that:

- Internal scrutiny must be independent and objective.
- Internal scrutiny must be conducted by someone suitably qualified and Experienced.
- A bought-in internal audit service could conduct internal scrutiny.



More about the RPA

RPA Cyber Risk Cover Eligibility Requirements

Applies to: All schools that are members of the DfE's Risk Protection Arrangement (RPA) for schools.

The RPA is an alternative to commercial insurance offered by the Department for Education.

In order to be eligible for the cover, schools must meet the Conditions of Cover.

Conditions of Cover

- All members must meet the Department for Education's Cyber security standard relating to backups.
- All employees or governors who have access to the member's information technology system must undertake NCSC training annually.
  - Schools are required to evidence all staff and board member completion of this training in the event of a claim, so all records of completion must be retained.
  - As the NCSC doesn't provide a way to evidence completion of the course, you should consider using a training provider.

Training available here

- All Members must have a Cyber Response Plan in place.
  - The DfE has made a template available on the RPA Risk Management portal. Alternatively, an interactive version is available on the Secure Schools Platform.
- All Members must register with Police CyberAlarm.
  - The condition is that each school registers with the Police CyberAlarm. You can register your school at: cyberalarm.police.uk
  - Your school's IT team is best placed to decide if the appliance is suitable and compatible.

Closing thoughts

From our engagements in the cybersecurity industry and the education sector, we're observing a shift of focus from traditional policy and technical solutions to investing in people and culture. Despite a growing acknowledgement of the importance of culture in cybersecurity, it's difficult to measure. This shift is something that we, at Secure Schools, support. Perhaps we'll even see some creative solutions this year that support these efforts!I'll leave you with some questions for you and your school to ponder, as you look ahead to the next academic year:

- Should we incorporate mindfulness into user IT tasks such as reading emails, making our staff stop and think before taking a potentially risky action?
- If all of our staff had more time to spend on reading each email, would we be less susceptible to phishing attacks?
- If so, should more IT teams take an active role in reducing the amount of noise and emails staff are receiving?

Thanks again for your time reading this year's Handbook. I hope it has made the actions and guidance you need to take for this upcoming academic year a little more manageable.

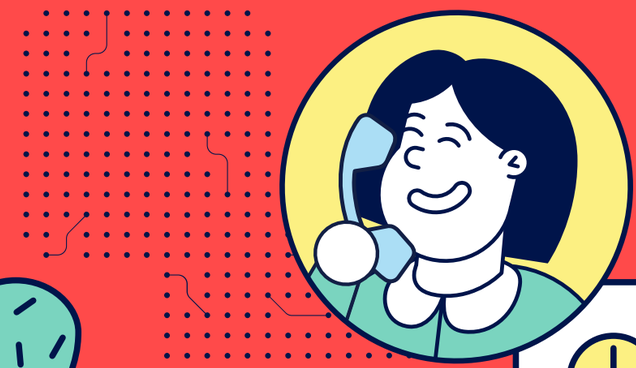
All the best,

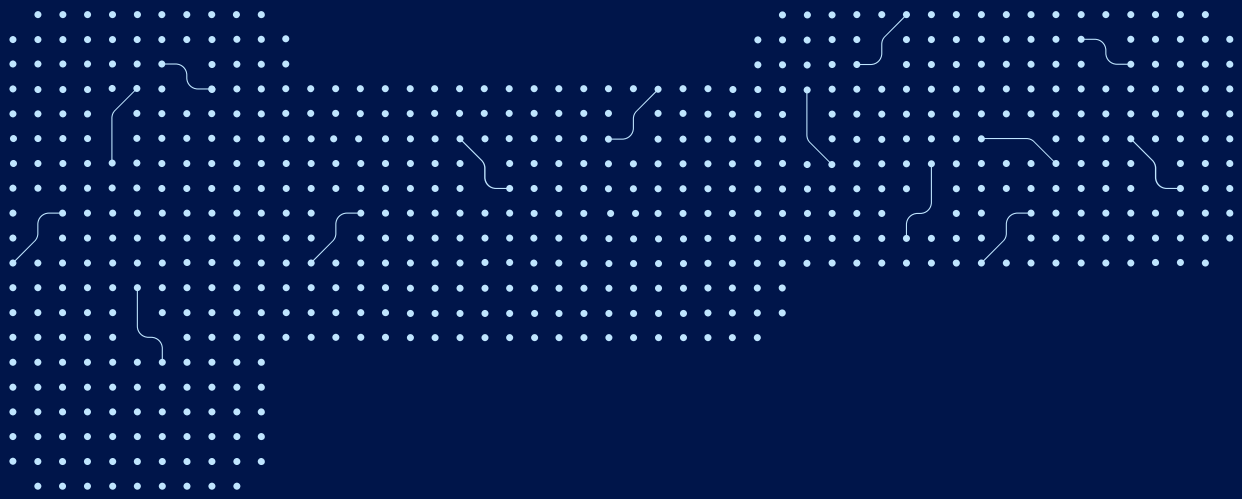
Paul Alberry

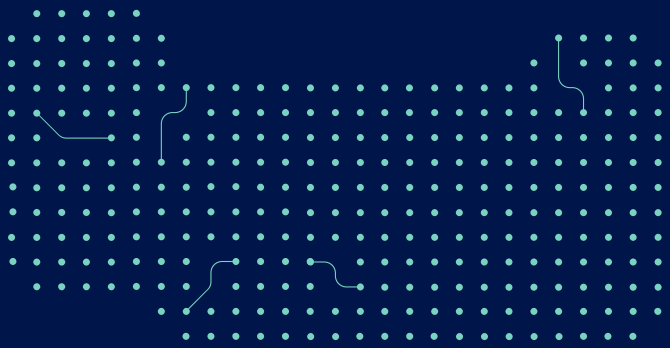
Co-founder and CEO
Secure Schools

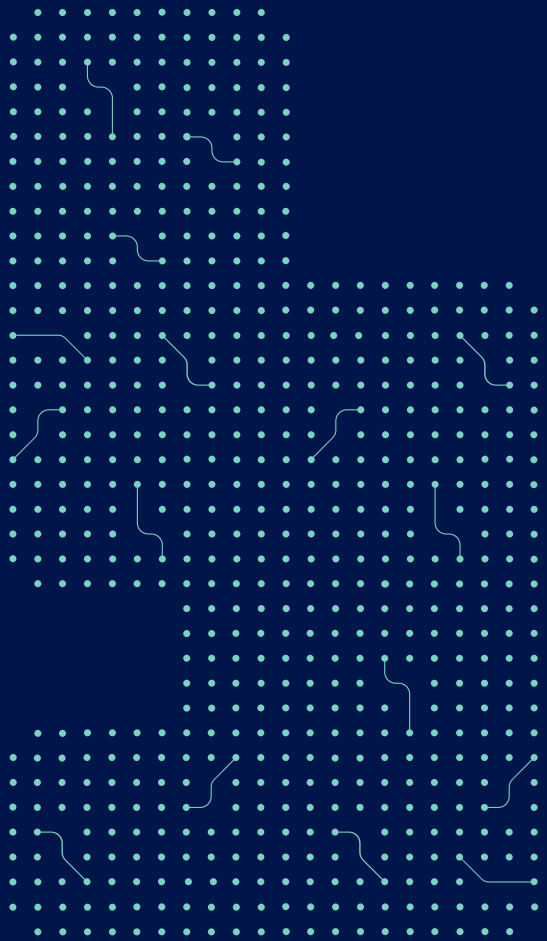
Try Secure Schools for 30-days for free

No obligations, no commitments – just 30 days of exploring how Secure Schools can reduce your school or trust's cybersecurity risk.









Secure Schools

secureschools.com

hello@secureschools.com

@secureschoolsuk