Governors' role in cyber security

Last reviewed on 22 July 2021 Ref: 39500

School types: All · School phases: All

Be clear on what you need to know about cyber security, and the questions you can ask your school leaders, so you can be assured your school is as safe as possible from a cyber attack.

Contents

Our thanks to the following experts for their help with this article: Karen Mitchell; Vickie Cieplak and Edward Trimbee from the West Midlands Regional Cyber Crime Unit; and our internal IT experts at The Key and ScholarPack.

We also refer to the National Cyber Security Centre (NCSC) and its resources throughout this article.

You're responsible for your school's cyber security

It's not just down to your school's IT department

In a similar way to health and safety and safeguarding, cyber security is the responsibility of the **whole board** – not just 1 person. This is because it's central to your school's ability to operate and function.

While your school leaders should work closely with your IT department to put precautions in place, it's up to you to monitor what your school's doing, and to make sure cyber security is given the time and resources needed to make the school secure.

This is explained on page 11 of the NCSC's board toolkit.

Make cyber security a priority for your school

Cyber security is becoming more important than ever, with many schools falling victim to cyber attacks, particularly ransomware attacks.

This article will show you where your school can get started.

Cyber security is important because:

- You and your school leaders are responsible for making sure you have the appropriate level of security protection and procedures in place. This is explained in paragraph 131 of Keeping Children Safe in Education
- School data is incredibly sensitive – if it's compromised, this can be a risk to the pupils in your care
- Everything in your school relies on your computer network. An attack could mean your school leaders:
  - Can't contact staff in an emergency
  - Can't pay their staff, caterers or other service providers
  - Lose students' coursework
  - Lose financial records and all their data
- Even if you did pay a ransom (which you should not), there's no guarantee you would get your data back

If you're an academy, remember to contact the Education and Skills Funding Agency (ESFA) before paying any ransom demands (this is explained in paragraph 6.17 of the Academy Trust Handbook).

What's ransomware?

It's a type of malware which stops you accessing your systems and the data held on them – your data could be encrypted, stolen or deleted, and you'll usually receive a ransom note demanding you make a payment to recover the data.

This is one of the biggest threats to schools, but it isn't the only one.

You should also be aware of phishing emails (used to release ransomware via a malicious link or file) as well as the potential for your own students to hack into your network. Get up to speed on various cyber security terms with our glossary, and get more support with what you need to know about ransomware with guidance from the NCSC.

Stay strategic

You don't need to suddenly become an IT expert and know the intricate details of how cyber attacks work, and you won't be expected to walk around your school with a checklist of what measures your school should have in place – but you can get up to speed on some terms so you feel a bit more confident when you chat to your school leaders about how they are addressing cyber security.

Your role is to:

- Make sure cyber security is part of your school's objectives and risks
  - Add cyber security as an agenda item for your next meeting. It's also a good idea to combine cyber security with things like GDPR and the school's physical security as a regular agenda item
  - Speak to your school leaders about adding cyber security to your school improvement plan (SIP)
  - Check that cyber security is included as part of your school's risk register
- Support your school leaders to put precautions in place
  - You need to be prepared to put your money where your mouth is and give your school leaders the time and resources to put updated systems and procedures in place – for example, to organise a cyber security audit
- Hold your school leaders to account to make sure they have in systems in place to keep your school secure
  - You'll do this by asking questions (which we cover in this article)

A good place to start is with the NCSC's board toolkit.

It's money well spent

Some elements of making your school cyber secure can be expensive (for example, replacing your IT software), but the alternative can be far more financially damaging, and a data breach could negatively affect the school's reputation and relationships.

As well as ransoms from hackers, your school could be investigated and fined by the Information Commissioner's Office (ICO) as a result of a data breach – so prevention is definitely better than cure.

Get support from your LA or trust

You don't need to tackle this all on your own.

Flag to your school leaders that they should speak to your local authority (LA) or trust first about what it can offer your school regarding cyber security – it may be able to advise you on what service providers to use, or may help in procurement.

Get training for you and your school's staff

This is a crucial part of protecting your school from cyber attacks.

From phishing emails to pressured phone calls, many attacks can succeed because of limited training.

Ask for training for your governing board

Governors as well as staff can be the target of a cyber attack, particularly if you're seen to have influence, and access to valuable assets and information.

This is covered on page 9 of the NCSC's toolkit for boards.

Make sure you and your school's staff are trained annually on the basics of cyber security

This is to keep you up-to-date on the latest threats and to refresh your knowledge about what to look out for. Cyber attacks are often spread by email, so basic safety precautions are your school's first line of defence.

Training is particularly important for defending your school against social engineering attacks, such as phishing and payment fraud.

Ask your school leaders whether your school's training covers:

- Checking the sender address in an email
- Responding to a request for bank details, personal information or login details
- Verifying requests for payments or changes to information

This is recommended on pages 13 to 15 of the Metropolitan Police's Little Book of Cyber Scams 2.0.

Make sure that your school leaders include cyber security training as part of induction for any new starters – this is especially important if they start outside of your school's annual training window.

We've covered these questions in our 'questions to ask' section below.

Free sources of training and support:

- **The National Cyber Security Centre (NCSC)**
  - Your school leaders can access cyber security training for school staff. Find out more here
  - Your school leaders can download your own cyber security information cards in English and Welsh and send these out to your staff
- **Your local Regional Organised Crime Unit (ROCU)** – it can work with your school to provide free cyber security advice and support so you can improve your awareness of, and defences against, cyber attacks
  - It can also deliver the Cyber Choices programme in your school to help students with cyber skills make the right choices

If your school leaders decide to find their own provider to deliver training for your staff, make sure:

- The training is school-specific
- The provider has experience in delivering training to schools
- They're clear on what will be covered in the training – make sure it covers areas such as data as well as phishing and ransomware
- Your school leaders know what staff should understand by the end of it

Your school leaders should have precautions in place

The controls your school has in place should be:

'Proportionate'

- It's difficult to provide a hard and fast way to tell if what your school has in place is 'proportionate', as it'll vary depending on your school size and what tasks people are performing
- The best way to work out whether what you've got in place is proportionate and working well is to get the specialists in, such as through a third party audit (which we cover further down this article). This is because they'll be able to objectively test what you have in place, and advise whether it's up to scratch
- Academies: the ESFA specifically notes that academies should have 'proportionate controls' in place against cybercrime – this is explained on page 58 of the Academy Trust Handbook

Multi-layered

- Everyone needs to be aware of cyber security risks – from your front-line staff to your wider supply chain, everyone needs to be clear on what to look out for to keep your systems safe

Up-to-date

- Running old, unsupported and out of date software can leave your system vulnerable

Regularly reviewed and tested

- Your school needs to make sure that its systems are up to scratch and as secure as they can be

Give me some examples

Below we've listed some examples of the types of precautions your school leaders could put in place.

Don't treat this as a checklist, self-review or audit – doing or arranging these things isn't your job.

Instead, use these prompts to help you ask questions about what your school leaders are doing to secure your school:

- **Annual staff training:** this should include refresher sessions/quizzes, and any updates to your school's reporting obligations/procedures
- **Updated systems and software:** your school shouldn't be running unsupported software like Windows XP or Windows 7
- **Regularly backed-up data:** your school's data should be backed up at least once a day, and stored on external hard drives that aren't connected to the school network. Let your school leaders know about specific guidance on backing up data here
- **A secure management information system (MIS):** your school leaders should be clear on who's responsible for maintaining the security of your school's MIS. It contains sensitive data, including pupils' names, medical records, safeguarding information and parent contact information
- **A virtual private network (VPN):** this is so staff working from home can dial in securely
- **Multi-factor authentication:** staff should enable multi-factor authentication where they can, on things like school email accounts
- **Regular access reviews:** this is where your IT department will make sure each user in your school has the correct level of permissions and admin rights. For example, if a pupil had permissions on their account to download software, this can leave your system vulnerable
- **A password manager:** to help staff store their passwords securely
- **A firewall in place:** this is to give your systems another layer of security
- **A secure supply chain:** your school leaders should have an idea of whether companies that supply your school are handling your information properly. Signpost your school leaders to guidance from the NCSC on making sure your supply chains are secure

Make sure your school leaders develop, review and test an incident response plan

They should do this with your IT department, and it should cover what procedures your school will follow in the event of a cyber attack.

For example, it should include how your school will communicate if communications go down, who they will contact and when, and who will notify Action Fraud of the incident.

Regarding governors, it should also cover:

- What your role is during an incident – this is because your chair might be involved with representing your school in the media
- Who you have delegated authority to
  - For example, who is responsible for escalating concerns, contacting the relevant authorities or taking down your website? (Make sure it includes incidents that happen outside of working hours too)
- When you want to be informed of the incident. Decide:
  - What significance of incident you want to be notified of
  - At what stage during the incident you want to be informed

This is covered on page 36 of the NCSC's toolkit for boards.

Your school leaders should review and test your school's procedures with your IT department:

- Annually (although ideally every 6 months)
- After a significant event has occurred

Ask to be involved when your school leaders test their procedures

This is so you can understand how an incident would impact your organisation, and how you would be involved.

This is recommended on page 36 of the NCSC's toolkit for boards.

To test your procedures, let your school leaders know about the NCSC's 'Exercise in a Box' to help you practise your response to a cyber attack.

Your school leaders might decide to organise an audit to coincide with the review of your procedures.

Ask your school leaders to organise an annual audit

This is the best way to know if your school systems are up to scratch.

Flag to your school leaders that they can speak to your LA or trust first about a potential provider – they may be able to give more bespoke guidance.

If it's up to your school to pick an auditor, make sure it chooses a third-party provider which:

- Specialises in cyber security
  - For example, if a third-party provider's website advertises lots of different IT services, it might not be a specialist in cyber security
- Has experience in cyber security auditing for schools
  - Schools aren't the same as corporations

An audit should assess what measures your school has in place and where any weaknesses are. It will then identify next steps you can take as a school to tighten up your cyber security.

You can expect an audit to:

- Include a request for your IT department to create your auditor a 'dummy' account, which they can use to check your school's security from different levels of user (e.g. to check that as a student user, they can't access anything they shouldn't)
- Conduct a penetration test ('pentest') – the auditor will try to penetrate your network to see how far they can bypass your systems
- Ask to see:
  - An overview of what systems you have in place
  - A risk assessment or incident response plan which covers your school's procedures if there were a cyber attack
  - An ICT strategy plan or similar (for example, if your school improvement plan (SIP) includes that you'll replace your computers, the auditor might ask to see this)
- Give your school some clear next steps to make your network more secure

Ask your school leaders to send the completed audit to your governing board

This is so you can have clear oversight of the process and ask questions.

Feel free to challenge anything you see on the audit. While you don't necessarily need to understand what type of firewall your school has, for example, you can question why it hasn't been put in place.

You should then work with your school leaders to feed the results of the audit into your school's priorities.

Questions to ask your school leaders

Ask these questions of your school leaders during full governing board or committee meetings. The questions below are from our experts or based on various sources from the NCSC.

Use these questions as a starting point, but remember that you don't need to ask them all in one sitting and you can add any other questions that you think are appropriate.

Find links to more questions you can ask at the bottom of this section.

Tell me about what precautions you have in place to make the school more secure

How do you monitor whether the systems our school has in place are effective?

How often do staff receive training in cyber security? What does this training cover? How do you know it's effective?

What cyber expertise do we need, and what do we already have?

How do you back up the school's data? Are you confident it would remain unaffected if we had a ransomware attack?

When did you last organise an audit which looked at cyber security specifically?

Do you have an incident response plan in place? Is it up to date? How do you know it's effective? Do you know who to contact if our school becomes the victim of a cyber incident?

What does our school do to encourage a good security culture?

How do you keep track of all the systems and data that you're responsible for?

If you're notified of an incident and/or security breach, ask: 'How did this happen?'

Be sure to follow up with: 'What will you do to reduce the likelihood of an incident like this happening again?'

More questions you can ask

To see more questions you can ask, including some of the ones used in this article, take a look at the following resources:

- Cyber security in schools: questions for governors and trustees
- NCSC board toolkit
- Ransomware: what board members should know and what they should be asking their technical experts

Free resources for your school

Below we've listed all the resources mentioned in this article, plus some additional links, which you and your school leaders can use to make your school more cyber secure. Your school leaders should work with your IT department to see what would work best for them.

Resources for you

- Questions for governors and trustees
- NCSC board toolkit
- Ransomware: what board members should know and what they should be asking their technical experts

Resources for your school leaders

- Cyber Security for Schools
- Cyber security information cards
- 10 steps to cyber security (medium and large organisations)
- Small Business Guide: Cyber Security (small organisations)
  - Use the NCSC's checklist of actions you can take
- Little Book of Cyber Scams 2.0

- Offline backups in an online world

Tools, training and support for your school leaders:

- Police CyberAlarm – this is a tool which can help your school understand and monitor malicious cyber activity
- Early Warning service from the NCSC – this service will inform your organisation as soon as possible of a potential cyber attack on your network
- Cyber Essentials certification – this is a government-backed scheme from the NCSC that will help to protect you from the most common cyber attacks. Your school can achieve 2 levels of certification – find out more here
- Cyber security training for school staff
- Your local Regional Organised Crime Unit (ROCU) – it can work with your school to provide cyber security advice and support so you can improve your awareness of, and defences against, cyber attacks
  - It can also deliver the Cyber Choices programme in your school to help students with cyber skills make the right choices
- Your school leaders can carry out a self-review of your online safety procedures with this free tool from 360 degree safe

Sources

Vickie Cieplak is cyber protect, prepare and prevent officer, and Edward Trimbee is detective sergeant, at West Midlands Regional Cyber Crime Unit. Funded by the National Cyber Security Programme, the unit delivers free cybercrime policing support to the public and private sector in its region. You can contact them via email: wmcyber@west-midlands.pnn.police.uk

Karen Mitchell has spent much of her career working in local authorities providing ICT and information management support services to schools. She now works as an independent consultant in the school sector and is vice chair of the resource committee on a school governing board.

Next steps

- Cyber security glossary

Also in this topic: Data protection and the GDPR

- Cyber security glossary
- GDPR cheat sheet: how to keep personal data safe
- GDPR glossary
- GDPR: personal data breach procedure
- GDPR: what governors and trustees need to do to be compliant
- **QuickRead:** The UK GDPR
- UK GDPR: Questions to ask your DPO

Show more

Top articles

- Cyber security glossary
- GDPR: what governors and trustees need to do to be compliant
- Governors' role in cyber security
- **QuickRead:** The UK GDPR