INFORMATION

Cyber security in schools: questions for governors and trustees

Questions for the governing body and trustees to ask school leaders, to help improve a school's understanding of its cyber security risks.

Schools rely heavily on IT and online services to function. They also hold large amounts of sensitive personal data on pupils, parents and staff. All this needs to be kept safe and secure.

What is cyber security and why it matters to schools?

Cyber security is about protecting the **devices** we use, and the **services** we access online from theft or damage. It is also about preventing unauthorised **access** to the vast amounts of personal data we store on these devices and in online accounts.

A cyber security incident can affect the school's ability to function, the security of its data and its reputation. Both the school leaders and the governing body will want to ensure they are aware of cyber risks and adequately prepared in the event of a cyber incident. Schools will already be following similar approaches when it comes to managing risks and responsibilities around GDPR and pupil safeguarding more generally.

Roles and responsibilities

The role of governing boards is strategic and should be focused on ensuring that the school or trust has IT policies and procedures in place that cover the use of ICT systems and data security, including compliance with the General Data Protection Regulations (GDPR).

8 questions for governors and school leaders, to start the cyber security conversation

The following 8 questions have been produced by the National Cyber Security Centre (NCSC) and the Department for Education (DfE), to help improve a school's understanding of their cyber security risks in a proportionate way. These questions are not intended as a checklist. They have been written to **start the cyber security conversation between the governing body *and* the school leaders**, with governing body taking the lead.

The questions are set out across three themes: to **seek out information**, **raise awareness**, and **improve preparedness** in case of an incident. We envisage these questions will then encourage further conversations between the school leaders and those that procure and/or manage the IT in the school.

Theme A: Information seeking

Factual questions by the governing body to give the school a good understanding of their IT estate:

1. Does the school have a list of the different organisations that provide its IT services?

For a school to keep its data and systems safe, it should know who its main IT providers are. This list might include **who provides the school's internet connection** or **who runs the school's website**. It might also cover IT support contracts from a **Local Authority** or a **Managed Service Provider**.

2. Does the school leader know who manages or coordinates the IT within the school?

Depending on the school, this may be a member of teaching staff, a dedicated network manager or an external provider.It's important the school leader knows who this is, and that this person/team/company follows key cyber security practices as outlined in the NCSC's guidance 10 Steps to Cyber Security and the Small Business Guide.

3. Has the school identified the most critical parts of the school's digital estate and sought assurance about its security?

Some digital services are critical to the day-to-day running of the school, these are the ones that will need securing the most. Think of them like the school's "crown jewels". For example, the school's Management Information System (MIS) will contain pupils' medical records, safeguarding information and parental contact information. Without access to these records (or hard copy backup), schools would find it difficult to remain operational if their IT went down. The IT services in your school could be managed internally or contracted out, or a mixture of both.

TIP: Asking the school to adhere to cyber security best practices when buying in IT services or managing IT teams within the school can provide the governing body with a level of assurance. The UK government's digital marketplace has a suite called G-Cloud where schools can procure cloud IT services and products. Products from this site will have a decent level of security already built in. Other cyber security best practices are outlined in the NCSC's guidance 10 Steps to Cyber Security and the Small Business Guide.

4. Does the school have a proper backup and restoration plan in place?

If a school loses access to its critical data, the effects can be softened by having a proper backup and restoration plan in place. Backups of important data can help when there are cyber incidents but also with other disaster scenarios like: fire, floods, physical damage or theft of devices.

TIP: To seek assurance, ask your school leader/s to ensure the school's IT team or provider backs up data in accordance with the NCSC's Small Business Guide. It is important that backups are kept segregated from the school's network and they can be easily restored. The school should **practice** restoring these backups regularly.

Theme B: Awareness

The degree to which both users and the governing body understand the importance of cyber security and their role in it:

5. Do the school's governance and IT policies reflect the importance of good cyber security?

TIP: Cyber incidents or attacks should be considered in terms of risk management and be listed on the school's risk register, alongside other IT and data risks. Cyber security should be referenced in any relevant school policies (e.g. business continuity, data protection, acceptable usage etc). It is also advisable to have cyber security as a regular agenda item at board meetings as with other topics like GDPR and the physical security of the school.

6. Does the school train staff on the common cyber security threats and incidents that schools experience?

Good cyber security is dependent on people. Staff can alert schools to potential problems like spotting phishing emails or phone calls, or noticing when a service is running particularly slowly, which could be a sign of a cyber attack.

TIP: Assurance can be sought by asking the school's staff to take part in cyber security training. Free training is due to be published on the NCSC's website in September 2020. There are other training resources like the Practical Tips guide which can be downloaded from the NCSC's website.

Theme C: Preparedness

Being prepared for the potential impact of a cyber security incident is crucial in helping schools minimise disruption should an incident occur:

7. If the school temporarily lost access to its data and/or internet connection would the school still be able to operate?

All types of schools can experience a cyber incident. A cyber incident could result in a school's network being unavailable for an unknown period of time, with limited or no access to important data and services. The importance of access to the MIS has been covered earlier in theme A, but there are other services like: telephones, access control systems, cashless payment systems. These will impact on the school's operation if they are unavailable.

TIP: Assurance can be sought in this instance by establishing whether the school has a business continuity plan in place, that includes IT and these wider services. For example, it might be that your school holds a paper copy of the school register and parent contact information. This way a school can increase its chances of functioning in the event of a cyber incident. Key to this is the list of IT service suppliers the school uses including contact numbers. The NCSC's 10 steps to Cyber Security and the Response and Recovery Guide can help inform the school and provide governors with assurance.

8. Does the school know who to contact if it becomes a victim of a cyber incident?

A school's business continuity plan should list its key external IT supplier/providers as well as those responsible for the management of IT within the school. It is very important that up-to-date contact information sits alongside this.

TIP: A school establishing what role these IT suppliers/providers will perform in the event of a cyber incident would be very beneficial at this planning stage. If additional support or expertise is needed in the event of an incident this should be identified beforehand. A school may also want to list important contact information from: the local authority, chair of the governing body and local law enforcement. Reporting cyber incidents can be made to Action Fraud or, if you're in Scotland, then reports should be made to Police Scotland. If the incident involved a data breach it may be necessary to report it to the Information Commissioner's Office (ICO) under GDPR guidelines.

For governing bodies who are responsible for large schools or trusts, or who would like to develop their understanding of cyber security at board level further; the NCSC has produced a board toolkit to help generate constructive cyber security discussions between board members and technical experts.

PUBLISHED

15 July 2020

REVIEWED

15 July 2020

WRITTEN FOR ⓘ

Small & medium sized organisations

Self employed & sole traders