Cyber Essentials Information for School Governors

How well could your school function if IT services were interrupted and the data lost?

From recording and reporting detailed performance data, to staff sharing content and collaborating with students, schools are increasingly reliant on computers and connectivity.

Like all organisations, following the pandemic, schools are making greater use of technology and the internet. It is vital that schools take all the steps they can to keep their systems, people, and data secure and safe from harm.

The Information Commissioner has advised schools to be particularly vigilant around information security. It has warned that unauthorised access to personal information would be particularly harmful to pupils, parents and staff; people with a right to seek compensation if the loss of their personal data caused them damage.

Under the Data Protection Act 2018 it is necessary for an organisation to evidence they are using 'appropriate technical and organisational measures'.

Cyber Essentials allows you to document and evidence compliance, to lower risk and protect your school.

What is Cyber Essentials?

Cyber Essentials is a UK government scheme supported by the National Cyber Security Centre (NCSC), and is intended to help organisations of any size demonstrate their commitment to cyber security. It is a straightforward way for your school or academy to improve its cyber security and understand the key controls which can be used to maintain a secure school.

Cyber Essentials provides a well-documented framework for a baseline in cyber security. The framework is designed to be clear and straight forward, and the wording is intended to support managers without technical knowledge.

What does it cover?

The scheme focuses on five key cyber security measures (also called controls), which are simple to put in place yet help protect organisations from up to 80% of cyber-attacks.

The Five Key Controls:

1. Firewalls - Secure your Internet connection
2. Configuration - Secure your devices and software
3. User Access - Control access to your data and services

4. Malware Protection – Prevent viruses and other malware
5. Patch Management - Keep your devices and software up to date

Governors should also consider the ‘human factor’ when looking at security. It is essential that schools also train **all** staff to be “cyber aware”.

Why Cyber Essentials?

Whatever the size of your school, trust or college, every organisation must start somewhere, and the basic yet effective controls described in the Cyber Essentials scheme are a good place to begin.

Achieving Cyber Essentials certification helps evidence your commitment to cyber security and documents the fact you have implemented effective protection.

The Strategic Role of Governors

Governors need to be actively involved in monitoring incidents and identifying risks in order to make strategic decisions.

The Governors handbook references cyber security, stating:

“A school or academy trust’s security policy or plan should also include an assessment of cyber security risk. A cyber security incident can result in a data breach where sensitive personal information on pupils, parents and staff is accessed without permission. This can have implications for safeguarding and can also result in serious disruption to the running of the school”

The National Cyber Security Centre (NCSC) also provides support for governors and trustees to ask crucial questions of school leaders.

It is vital that, as a governing body, you have oversight of any data protection breaches and IT incidents. Make sure your school has an incident reporting mechanism in place and that the culture is one of support and not one of blame.

Governor Actions

Cyber Essentials requires that you meet the key controls. For many schools these will already be in place but may need reviewing or documenting.

Cyber Essentials Information for School Governors

1. Schools need to define the ‘scope’ of their network for the assessment. A scope which covers the whole organisation is more secure.

2. Identify key staff who will be involved in providing support for the submission and ensure they have the resources to complete any necessary tasks.

3. If your school uses outsourced IT services / third-party technicians, you may need to consider how they can support the submission and whether there will be any impact on their usual tasks. This may have a short-term implication on cost.

4. The assessment may highlight old devices or systems which may need to be upgraded or replaced. Ensure there is a process for handling any purchase requests and add cyber security to your IT budget.

5. Ensure you schedule time to review and approve updated policies, and be aware that at least one member of the governing board will need to sign the Cyber Essentials final declaration document.

Further information about Cyber Essentials can be found here.