

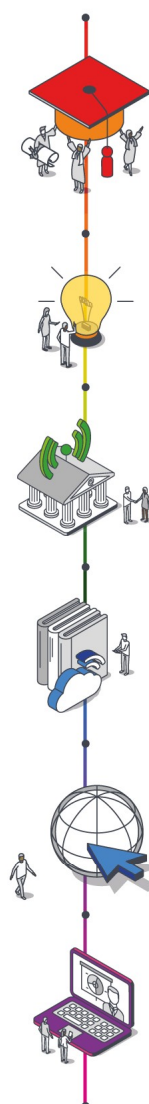
## Cyber Resilience Programme

As reliance on technology increases, so does the level of risk and attack frequency. Cyber Resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions on contested IT systems. Schools ICT have developed a three stage programme with our partner Secure Schools.

Our programme is designed to help all schools and academy trusts with improving their cyber resilience no matter their current position. This is achieved through auditing, scrutineering, certification and training.

### Key benefits of the service

- ✓ Become more Cyber Resilient!
- ✓ Support with auditing, planning, training and monitoring
- ✓ Gain confidence through out neutral analysis and independent assurance
- ✓ Programme designed for education, resourced by education experts
- ✓ Three stage programme, you set the pace and the risk appetite
- ✓ You decide how much of the programme you want to complete
- ✓ Aligned to DfE, ESFA, NCSC and IASME standards
- ✓ Option to obtain formal government-backed certifications
- ✓ Delivered as a confidential and supportive service
- ✓ Cost-effective compared to programmes offered commercially.



## The three stage programme - Audit, Improve, Assure

Starting with the first stage, you set the pace. Most effective as an ongoing cycle.

### Stage 1 - Audit

- Self-evaluation and triangulation audit of the intentions documented in the school or trust's policies, procedures and records
- Establishing the consistency in which academies follow these policies, procedures and records
- Receive a clear recommended action plan with prioritisation matrix to tackle 'quick wins'
- Access to cyber security awareness training and account breach monitoring.

### Stage 2 - Improve

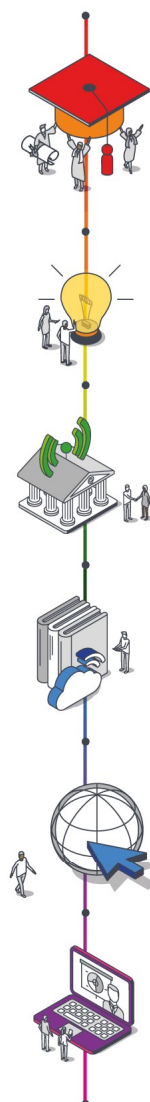
- Support in adapting documentation (policies, procedures and records) to align with the five technical controls of Cyber Essentials
- Begin planning the approach to completing the school or trust's Cyber Essentials application. Advice and support on how to align non-compliances.

#### Optional - Stage 2.1 - Cyber Essentials Certification Submission Attempt

### Stage 3 - Assure

- Scrutineering of networks, systems, devices and human factors such as the configuration of servers and endpoint devices to verify they meet the intentions set by the school or trust, security best practice and are ready for Cyber Essentials Plus Certification
- Testing of staff response to social engineering attempts, including USB drop and Phishing simulations
- Scanning for vulnerabilities existing at the IT network boundary and inside the school or trust's IT networks
- Penetration testing of the school or trust's wi-fi networks.

#### Optional - Stage 3.1 - Cyber Essentials Plus Certification Submission Attempt



Secure Schools Ltd is an NCSC Cyber Accelerator programme alumni and Cyber Essentials certification body

**More information is available on each programme stage upon request**

t. 01323 463133 e. [info@schoolsict.services](mailto:info@schoolsict.services) @SchoolsICTS [www.schoolsict.services](http://www.schoolsict.services)