Cyber Security Checklist for Schools

SWGfL
Safe. Secure. Online

A successful cyber attack has the potential to greatly impact upon an educational establishment. As education establishments continue to remain a target for attack they should ensure they put cyber and information security as the number one item on the risk register. Results from our 2022 Cyber Security in UK Schools report showed:

- 62% of schools had not received cyber security training
- 80% of schools had no air-gapped backup
- Almost a third had no IT security policy
- Small schools are more at risk
- 70% had no high-risk staff training in place
- 17% reported a cyber attack, 48% of which were ransomware

How Can You Protect Your School from Cyber Attacks?

Fortunately for schools, cyber security doesn't have to be as complicated as it may sound. The best thing to do is to take action now, to protect against some common threats. Take a look at the actions below and implement as many as you can.

Train your staff

1 Train regularly and not just once a year

2 Provide training around personal risks, not just organisational ones

3 Keep training interesting and engaging

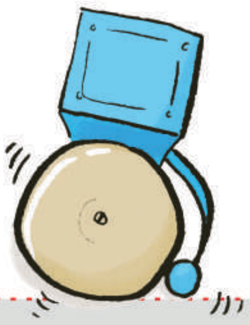
4 Identify those who may have access to sensitive information and provide additional training – headteacher, DSL, admin staff, office manager, business manager, HR lead.

Expect an attack

1 Attacks happen all the time and can target anyone so always be ready!

2 Encourage vigilance and praise staff when they report an issue, event or suspicious behaviour.

3 Use technology to help – monitor logs, keep software updated, use endpoint protection, scan incoming emails - use what you have to maximum effect



Write an emergency plan

1 Record what you will do, when, how and by whom if an attack happens – it is easier to react if a plan is already in place.

2 Record key contact details, login details to key systems and other information you might need if you couldn't access anything in your organisation.

3 Plan for a range of likely events that can affect your school's data such as ransomware, internet outage or fire.

4 Keep the plan in a safe, secure, yet accessible place – not on the premises

Backup (and test) your data

1 Backup all the critical data you need to keep safe and secure.

2 Test that the backups work

3 Take a copy of the back up monthly onto a removeable device and store it somewhere safe – this is a basic air-gapped solution. If you can, have multiple removeable devices and rotate their usage.

To find out more about our cyber security products and services visit: https://swgfl.org.uk/security/

or scan the QR code

SWGfL
Safe. Secure. Online

mimecast

Bitdefender
BUILT FOR RESILIENCE