You may have seen in recent press reports that school data and networks are being targeted and attacked by cyber security hackers. There have been some very public security attacks and even smaller scale attacks which have caused significant disruption to working practices.

What normally springs to mind is the bad publicity and financial implications of such an incident. However, there are also other impacts as attacks will normally involve data being temporarily or permanently deleted. You could be without access to work and teaching documents for a period of time, meaning part of your school could come to a standstill. You may also need to report these breaches to the data protection regulator, the Information Commissioner's Office.

You cannot safeguard against every possibility but it is important to be vigilant as some attacks are preventable. We have compiled a list of tips which you can take now to minimise the impact of cyber security threats: -

1. **Think before you open**: Don't get hooked in by emails providing unexpected promises. If it seems too good to be true, it probably is. Viruses, malware and data fraud can all arise from opening contaminated links or providing data to an unsecure area of the web.

2. **Don't open links**: Unless you can be 100% satisfied of the source. Consider whether it may be better to type the link out into your browser if you are unsure.

3. **Beware of urgent emails:** Attackers will target vulnerability requiring you to act immediately, usually with the threat of financial implications if you don't. Don't forget the attacker wants you to act without thinking or to make you feel like you have done something wrong.

4. **Verify:** If you are not sure where an email has come from, take steps to verify their credentials before opening. For example, try googling the web address or calling the company to verify the email address is correct.

5. **Investigate:** Phishing emails are getting more and more effective at finding ways to catch you out - but that doesn't mean that clues aren't left. Areas to watch out for range from bad spelling, new account details for payments, vague details and strangely titled attachments and links.

6. **Passwords:** Passwords should have, as a minimum, a complexity requirement (for example a certain number of characters as well as a mixture of numbers, letters and special characters). If users have a long and strong password, it makes it more difficult for an attacker to access that account.

7. **Approved devices:** Avoid plugging in your own memory stick or hard drive onto the school network as these can be sources of infection and risk. If you really need to use your own device, seek approval from your school before use.

8. **Approved software**: Only use software provided by your IT department. Never attempt to install software downloaded from the internet yourself.

9. **Screen lock**: Whenever you leave your computer, even for a short time, always apply the screen-lock.

10. **Shut down**: Always shut down your computer at the end of the day as it allows the system to install important updates.

Under GDPR it is the school's responsibility to ensure appropriate security for personal data. This includes protection against unauthorised or unlawful processing as well as against loss or destruction of data. The above are all examples of how to minimise this risk.