Cyber Security
Top Tips to Help You Protect Your ICT and Your Data

A recent 2024 DSIT report highlighted that 71% of secondary schools and 52% of Primary schools in their study identified a breach or attack in the past year. To help schools in planning their ICT Infrastructure, we've pulled together a list of tips that will help your school protect itself, lessen the chance of a successful cyber-attack and help you to be prepared should one occur:

1 Read guidance available from the DfE published in May 2024 "Cyber Security Standards for Schools and Colleges".

2 The National Cyber Security Centre (NCSC) provide free cyber-security training resources for schools and lots of other useful guidance for schools. Try this self-learning video for school staff.

3 Consider the impact a cyber-security incident might have on your school and develop your school's response as part of your business continuity planning. Consider whether you require cyberattack insurance cover, to cover restoration costs from specialist providers and check your support contracts. Our SIMS Managed Service option and Technical Support Visits for Curriculum Network can provide some assistance in the event of a cyber-attack (see details in the Service Definitions).

4 Plan for ongoing ICT investment – old, out-of-date technology and systems are a higher security risk and their slow performance will negatively impact pupils learning experience and the efficiency of school staff.

5 Make sure every server, laptop and desktop have anti-virus/threat protection software installed (don't be tempted to remove from older devices to make them run faster).

6 Make sure you have adequate backups of all systems and important sensitive data, preferably including dual off-site, encrypted backups with built-in malware protection, so your IT support can recover data if needed.

7 Train staff on how to recognise phishing emails and not to click on links in them (this is still one of the most common ways used to attack ICT systems).

8 Ensure accounts with high levels of access to systems are securely controlled and kept to a minimum and that all accounts accessing sensitive information are unique and secured with MFA.

9 Protect staff, parents, governors, and pupil identities online by ensuring everyone uses a unique identity as their username (with MFA enabled) when logging into systems containing personal data (don't use or share generic email addresses to login).

10 Protect pupils online with web filtering and safeguarding tools for monitoring and alerting.

11 Increase everyone's understanding of good ICT security and working practice.

Learn about
Online Safeguarding here

CONTACT US NOW FOR MORE INFORMATION

educationdigitalservices@lancashire.gov.uk | 0300 123 6797 (Option 2)
www.educationdigitalservices.lancashire.gov.uk