Welcome to the May 2020 Scomis Online Safety Newsletter for Schools

Cyber Security for Schools

Is your School's data safe?
Increasing numbers of schools and colleges are being seriously impacted by cyber incidents:
phishing attempts to steal money and passwords
ransomware attacks that encrypts files preventing access

Why?
• Many cyber incidents are untargeted, affecting any school that doesn't have basic levels of protection.
• Schools hold large amounts of confidential, sensitive information including medical details about students, safe-guarding records, staff and parents' bank details. ***All this data should be kept safe, secure and protected by schools.***
• Cyber criminals want to make money. Organisations might be prepared to pay a ransom to get the information back.

Who is behind cyber attacks?

- Online criminals
- Hackers
- Malicious Insiders
- Honest Mistakes
- School Pupils

Some simple steps can make a huge difference:

- Never ignore software updates
- Staff should always lock devices when not being used
- Staff should not share accounts with others
- Only download apps and software from official app stores like Google Play or Apple's App Store

Remember! If it looks strange, get a second opinion
Visit the National Cyber Security Centre's website to access more advice including:

- Top Tips for Staff
- Small Business Guide
- Specific guidance on password
- Guidance on ***Phishing***

How to spot and report Phishing

Phishing 'flags':
Educate your users!

- Does the email contain poor quality images of logos?
- Are there spelling or grammatical errors?
- Does it the email address you as ***'dear friend'*** rather than by name?
- Does the email request urgent action?
- Does it refer to a previous message you don't remember seeing?

Check the NCSC's 5 technical controls you should put in place today, explained without jargon.

FIVE TECHNICAL CONTROLS

Reporting: If your school suffers a cybersecurity incident or is affected by fraud (e.g. money lost as a result of a phishing email or your IT systems are compromised). Notify your:

- IT Support
- Broadband Supplier

And report it to Action Fraud by calling 0300 123 2040 or go to www.actionfraud.police.uk

Video Conferencing

The Information Commissioner's Office has produced advice you can share with your staff to ensure they can communicate with confidence during these challenging times:

- Have you checked the privacy and security settings?
- Have you checked your organisation's policy?
- Is all your software up to date?
- Are you using the right tool for the job?

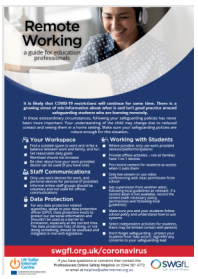
SWGfL—Video Conferencing for kids

Have you considered:

- How your personal data is protected?
- How children's data is considered by the platforms?
- If there are minimum age requirements?

SWGfL has collated and compiled some of the technical and policy details published by each of the services so you can more easily see which of these are the most suitable for you.

Access factsheets on:
Microsoft Teams / Skype
Google Meet / Hangout
Webex
GotToMeeting
Adobe Connect
Zoom
BlueJeans



Also read SWGfL's guidance on Safe Remote Learning

Free Safeguarding Software until September 2020

Online Safeguarding Software Companies CPOMS and My Concern are offering their products **free of charge** to schools not currently using their products until September

Free Webinars

Free Webinars from DfE Ed-Tech Demonstrator School
Staying Safe with Online Schooling 2nd June
Engaging and Supporting Parents in a Digital World 4th June
Both events are from 14.30pm to 16.00pm
Please click here for full details of these events and how to book.

Remember! Helpline for staff solely dedicated to supporting the children's workforce:
The Professionals Online Safety Helpline (POSH):
Website Tel: 0344 381 4772

For more information contact Scomis:
E: scomis@devon.gov.uk
T: 01392 385300

SCOMIS Your ICT Partner