National Cyber Security Centre
a part of GCHQ

NEN
The Education Network

Cyber security in schools:
Practical tips for everyone working in education

School Cyber Security

Each school needs to look after its data as well as manage the risks of using networked computers and services, and so **everyone needs to follow some basic principles of good cyber security as outlined in these cards**.

Senior leaders and governors need to be aware that cyber security is a management and assurance issue. After all, poor cyber hygiene could affect a school's ability to function, its reputation and its legal obligations to keep personal data safe.

*Cyber security is about protecting the **devices** we all use and the **services** we access online - both at home and work - from theft or damage.*

*It's also about preventing unauthorised access to the vast amounts of **personal information** we store on these devices and online.*

Why cyber security matters to schools

An increasing number of schools and colleges are being seriously impacted by cyber incidents: perhaps a phishing attempt to steal money and passwords, or a ransomware attack that encrypts files preventing access. But why?

- **Many cyber incidents are untargeted.**
  They can affect any school that doesn't have basic levels of protection.

- **Schools hold plenty of sensitive information.**
  For example, staff and parents' bank details, medical information about students, safeguarding records. All this has to be kept safe and confidential.

- **Cyber criminals want to make money.**
  They understand that an organisation's information is often sufficiently important to that organisation that they might be prepared to pay a ransom to get it back.

Who is behind cyber attacks?

Online criminals

Are really good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.

Hackers

Individuals with varying degrees of expertise, often acting in an untargeted way - perhaps to test their own skills or cause disruption for the sake of it.

Malicious insiders

Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest Mistakes

Sometimes staff, with the best intentions just make a mistake, for example by emailing something sensitive to the wrong email address.

School pupils

Some students simply enjoy the challenge of putting their cyber skills to the test.

Powerful Passwords

When implemented correctly, passwords are a free, easy and effective way of helping to prevent unauthorised users accessing devices or networks. Here's how to use them well:

- Have a different password for each account / service. If this isn't possible then make sure your most sensitive accounts (e.g. access to student records) have a unique password.
- If you **must** write down your passwords, store them securely and away from your device.
- Consider using a password manager – or ask your IT team whether this is an option.
- Use two factor authentication (2FA) on sensitive accounts. This gives a way of double-checking you really are who you are claiming to be.
- Always lock your account when you step away or stop using your device, even if it's just for a minute. This applies in school or when working from home.

A good way of creating a strong and memorable password is to use three random words. Have a look on the NCSC website to see why this is so effective.

Passwords should be easy for **you** to remember but hard for **somebody else** to guess. We recommend that you **don't** include the following:

- Partner's name
- Child's name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team
- A list of numbers (e.g. 123456) or words like 'password' or 'qwerty'.

What do people know about you?

What might they guess you'd use as a password? Try asking them. You might be surprised.

Watch out for phish!

In a typical phishing attack, scammers send fake emails to thousands of people asking for sensitive information (such as bank details) or containing links to bad websites. They do this to steal your details to sell or perhaps to access your organisation's information.

Reducing phishing emails needs to happen at different levels – we've got guidance for IT teams on our website - but all users should follow these guidelines:

- **'If in doubt, call it out'**. Always ask for advice if you're not sure if the link or email is legitimate.
- Don't feel silly if you think you have been caught out: it happens to all of us from time to time. But **do report this** to your Head Teacher or IT team so they can minimise any damage.
- Learn about **common phishing techniques**. (see overleaf)

Phishing flags

Some phishing emails are more sophisticated than others, but it helps to be aware of some of the more obvious clues. These include:

Does it contain poor quality images of logos?

Are there spelling or grammatical errors?

Does it address you as 'dear friend' rather than by name?

Is it asking you to act urgently?

Does it refer to a previous message you don't remember seeing?

USBs or Pen Drives

USBs are a helpful way to move data **but they can also spread viruses and malware from one computer or network to another.**

You might want to consider other ways of transferring data that offer greater security, e.g. saving work to an online storage provider or emailing it to yourself.

But if you must use a USB, do so with care.

- Only use USBs that you've been provided with by your school. Play it safe and don't use your own or any freebies you've been given.
- Make sure the USB is password protected. This means the data stored on it will be encrypted so can't be accessed if the USB is lost or stolen.
- If there is an option to 'autorun' programmes from the USB, make sure this is switched off so files have to be checked first.

Working from home

You're still responsible for keeping work information safe when you're accessing it at home. These tips can help to minimise the chances of any cyber security incident transferring from home devices to the school network or vice versa.

- Use up-to-date anti-virus software on your own devices.
- Download all software updates as soon as they are offered.
- Ensure **all** your devices have passcodes. (Even if you only use your laptop for work, for example, this may be synched to your phone or tablet).
- Change any default passwords on devices or software – including your home Wi-Fi.
- Switch on two-factor authentication (2FA) for sensitive accounts. Ask your IT department if this doesn't seem to be an option.

There's plenty more advice available on our website:

Top Tips for Staff our e-learning package to help you learn how to keep safe online.

The Small Business Guide is packed full of simple, actionable steps to reduce your chance of becoming a victim of a cyber incident at work or at home.

Specific guidance on **passwords** and **phishing** is available at www.ncsc.gov.uk

For whoever manages your school's IT:

Cyber Essentials - five key controls to guard against common cyber threats.

Ten Steps to Cyber Security - takes things a little further: breaks down the task of defending networks into ten essential components.

Exercise in A Box – a live tool that offers table-top and simulated exercises to practice on and learn from.

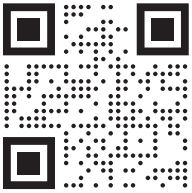
Reporting:

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), report it to ***Action Fraud*** *by calling 0300 123 2040 or go to www.actionfraud.police.uk or in Scotland through Police Scotland's 101 call centre*

Cyber Security Made Simple

Simple steps can make the world of difference, so don't forget:

- Never ignore software updates – they contain patches that keep you and your school secure
- Always lock your device when you're not using it
- Only download apps and software from official app stores like Google Play or Apple's App Store
- Don't share accounts with others
- Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of doing your work doesn't work!
- Create a culture of questioning – if it looks strange, get a second opinion



All advice is based on NCSC guidance as of August 2019. For print-ready files of these cards, please visit:
www.ncsc.gov.uk/information/resources-for-schools

@ncsc

National Cyber Security Centre